NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

AUTONOMOUS AND CONNECTED VEHICLES: A LAW ENFORCEMENT PRIMER

by

Jerry L. Davis

December 2015

Thesis Co-Advisors: Lynda Peters
                                              Kathleen Kiernan

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

13. ABSTRACT (maximum 200 words)

The introduction of autonomous and connected vehicle technologies will have a significant impact on ground transportation systems in the United States. Law enforcement agencies, legislative bodies, judiciary members, and regulatory bodies across the country will have to make changes in their operational, legislative, and regulatory processes to respond to incidents or events involving these technologies to ensure public safety mandates are satisfied. This thesis examined both technologies to gain an understanding of how they function and to identify by predictive analysis the emerging issues that will impact homeland security, as these systems could potentially be used for nefarious purposes. Securing the technology from cyber intrusion will be of paramount concern to manufacturers and consumers. An examination of a cyber security project to protect police vehicle fleets, undertaken by the Virginia State Police and University of Virginia, will highlight vulnerabilities and offer relevant recommendations to safeguard those assets. This thesis is intended to serve as a primer for law enforcement managers to develop a baseline understanding of autonomous and connected vehicle technology, while stimulating a re-examination of law enforcement roles and responsibilities that will require change as these technologies emerge.

THIS PAGE INTENTIONALLY LEFT BLANK

**AUTONOMOUS AND CONNECTED VEHICLES: A LAW ENFORCEMENT
PRIMER**

Jerry L. Davis
Captain, Division Commander, Bureau of Criminal Investigation,
Virginia State Police, Wytheville, Virginia
B.S., Troy State University, 1987

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2015**

Approved by: Lynda Peters
Thesis Co-Advisor

Dr. Kathleen Kiernan
Thesis Co-Advisor

Erik Dahl
Associate Chair of Instruction
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The introduction of autonomous and connected vehicle technologies will have a significant impact on ground transportation systems in the United States. Law enforcement agencies, legislative bodies, judiciary members, and regulatory bodies across the country will have to make changes in their operational, legislative, and regulatory processes to respond to incidents or events involving these technologies to ensure public safety mandates are satisfied. This thesis examined both technologies to gain an understanding of how they function and to identify by predictive analysis the emerging issues that will impact homeland security, as these systems could potentially be used for nefarious purposes. Securing the technology from cyber intrusion will be of paramount concern to manufacturers and consumers. An examination of a cyber security project to protect police vehicle fleets, undertaken by the Virginia State Police and University of Virginia, will highlight vulnerabilities and offer relevant recommendations to safeguard those assets. This thesis is intended to serve as a primer for law enforcement managers to develop a baseline understanding of autonomous and connected vehicle technology, while stimulating a re-examination of law enforcement roles and responsibilities that will require change as these technologies emerge.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AASHTO	American Association of State Highway and Transportation Officials
APL	Johns Hopkins Applied Physics Laboratory
AV	autonomous vehicle
BMW	British Motor Works
CA	certificate authority
CAN	controller area network
CD	compact disk
CV	connected vehicle
DARPA	Defense Advanced Research Projects Agency
DB	Digital Bond Labs
DCJS	Department of Criminal Justice Services
DEA	Drug Enforcement Administration
DHS S&T	DHS Science and Technology Directorate
DHS	U.S. Department of Homeland Security
DMV	Department of Motor Vehicles
DOD	Department of Defense
DoE	Energy Department
DOT Volpe	U.S. Department of Transportation Volpe Center
DRG	dynamic route guidance
DSRC	dedicated short range communication
DSSS	driving safety support systems
DVI	driver vehicle interface
ECU	electronic control unit
ETC	electronic toll collection
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FFRDC	Federally Funded Research and Development Center
FHWA	Federal Highway Administration
FMCSA	Federal Motor Carrier Safety Administration
FMEA	failure modes and effects analysis
FY	fiscal year
GHz	giga-hertz
GM	General Motors
GPS	global positioning systems
GSA	General Services Administration

HMI	human/machine interface
HTF	highway trust fund
IACP	International Association of Chiefs of Police
IC3	Internet Crime Complaint Center
ICS	industrial control systems
IIHS	Insurance Institute for Highway Safety
IOT	Internet of Things
ISAO	Information Sharing Analysis Organization
ITE	Institute of Transportation Engineers
ITS America	Intelligent Transportation Society of America
ITS	intelligent transportation systems
km/h	kilometers per hour
MAP-21	Moving Ahead for Progress in the 21st Century
mph	miles per hour
MSi	Mission Secure, Inc.
MTC	Mobility Transformation Center
NASA	National Aeronautics and Space Administration
NHTSA	National Highway Traffic Safety Administration
OBD	on board diagnostic
OEMs	original equipment manufacturers
OOS	out of service
PKI	public key infrastructure
RA	registering authority
RFID	radio frequency identification
SAE	Society of Automotive Engineers
SDV	self-driving vehicle
USB	universal serial bus
US-CERT	United States computer emergency readiness team
USDOT	U.S. Department of Transportation
UVA	University of Virginia
UWB	ultra-wideband
V2I	vehicle to infrastructure
V2V	vehicle to vehicle
V2X	vehicle to personal communication devices
VANET	vehicle ad hoc networks

VCTIR	Virginia Center for Transportation Innovation and Research
VDOT	Virginia Department of Transportation
VSP	Virginia state police
VTTI	Virginia Tech Transportation Institute

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Throughout the existence of man, there have been creations that have intertwined themselves in every facet of the human experience. Those that immediately come to mind and have evolved over centuries to the benefit and sometimes the chagrin of society include electricity, medicine, and weaponry of every description. The preeminent creation that has resulted in the expansion of nations and world economies would no doubt be transportation.

Specifically, the automobile has revolutionized ground transportation since its inception and its evolution continues today. From the Model T Fords of the early 20th century to today's complex vehicles with automated systems, the motor vehicle is entering a period of unprecedented change replete with enormous challenges.

Autonomous and connected vehicles are emerging technologies that have generated extreme interest in the safety community, the general public and governmental agencies responsible for regulation. These technologies are under study across the nation by academics, government, and private sector corporations and are likely to have a transformative effect on the entire ground transportation system.

This thesis will examine the evolution of a nationwide Intelligent Transportation System (ITS) to be created by the deployment of autonomous and connected vehicle technology. A brief examination of the rationale for an intelligent system will be offered along with a general overview of the associated technologies. Insights into the similarities and distinct differences between the two technologies will also be outlined.

These new technology systems rely heavily upon the wireless transmission of data and communications and as a result, a high priority will be placed on securing networks from breach. Law enforcement officials can ill afford to limit cyber protections to just their information systems. Physical systems, such as police vehicle fleets operated nationwide have potential vulnerabilities that must be understood and protected from cyber attack. The thesis will highlight this problem area and discuss in detail a recent

cybersecurity project undertaken by the Virginia State Police and the University of Virginia to address security of law enforcement fleet vehicles.

The findings from this thesis establish a baseline understanding of the technologies and establish functional recommendations for future research initiatives. All arenas intersecting with transportation will need to be re-evaluated with respect to the introduction of autonomous and connected vehicle technology.

Even tangential areas like public transportation, public policy, politics, along with environmental impacts, and land use planning will be affected as the technology is rolled out incrementally for consumer purchase. The cascading effects of change are multi-disciplinary and should be thoroughly evaluated by careful consideration of what potential unintended consequences may develop.

By virtue of the possible impacts on homeland security by the deployment of both technologies, law enforcement agencies, legislative bodies, judiciary members, and regulatory agencies across the country at all levels of government must be informed about this issue. Each entity will need to re-evaluate their operational, legislative, and regulatory processes in light of the complex changes wrought by an intelligent transportation system. These complex changes may affect statutory law, policy and agency response to incidents or events involving autonomous and connected vehicles.

It is believed that the thesis will serve as a law enforcement primer to educate police chiefs, sheriffs, and state police superintendents across the nation on this emerging technology. The reader will be exposed to the technology and have a basic understanding of the principles of autonomous and connected vehicle technology, while simultaneously exploring the homeland security related issues of concern. Having a fundamental understanding of the technology and system components is required of policy makers, law enforcement officials, and legislators in order that future regulation and policy decisions can be crafted effectively without stifling innovation.

ACKNOWLEDGMENTS

THIS PAGE INTENTIONALLY LEFT BLANK

I.   INTRODUCTION

Autonomous and connected vehicles are emerging technologies that have sparked interest among traffic safety advocates and are being touted by federal regulatory agencies like the National Highway Traffic Safety Administration (NHTSA) as being transformative for our transportation system.[1] These technologies are under extensive study across the nation by academics, government, and private sector corporations with the hope that both will be operational in the United States in the not too distant future.

Within the next five to 10 years, it is anticipated that autonomous vehicles will likely be available for purchase by the public. Nissan Corporation's Chief Executive Officer Carlos Ghosn has established the goal of marketing the first semi-autonomous car in 2020.[2] This technology is not limited to automobile manufactures; private sector corporations like Google have been developing their own version of autonomous vehicles since 2009 with accumulated mileage estimates exceeding 1,000,000 accident free miles while in the autonomous mode.[3] Delphi, a global supplier of automotive technology, recently completed a nine-day 3,400-mile cross-country demonstration of their autonomous vehicle technology.[4]

Connected vehicle technology is rapidly being developed and will provide safety critical data to drivers to make them more fully aware of the vehicle's dynamic environment. This technology may be mandated by NHTSA in new production vehicles, which could potentially enter the market as soon as 2019.[5] However, there are public

---

[1] NHTSA, *Planning for the Future of Transportation: Connected Vehicles and ITS* (Washington, DC, NHTSA, 2015), http://www.its.dot.gov/factsheets/pdf/PlanningFutureTransportation_FactSheet.pdf.

[2] "HowStuffWorks 'How Driverless Cars Will Work,'" accessed July 6, 2014, http://auto.howstuff works.com/under-the-hood/trends-innovations/driverless-car.htm.

[3] Chris Isidore, "Injuries in Google Self-Driving Car Accident," *CNNMoney*, July 17, 2015, http://money.cnn.com/2015/07/17/autos/google-self-driving-car-injury-accident/index.html.

[4] "Delphi Drive," accessed July 14, 2015, http://delphi.com/delphi-drive.

[5] "U.S. Department of Transportation Announces Decision to Move Forward with Vehicle-to-Vehicle Communication Technology for Light Vehicles," accessed July 28, 2014, http://www.nhtsa.gov/About+ NHTSA/Press+Releases/2014/USDOT+to+Move+Forward+with+Vehicle-to-Vehicle+Communication+ Technology+for+Light+Vehicles.

safety concerns raised by the introduction of these two technologies as they could be used by criminal elements.[6]

This thesis will examine the evolution of a nationwide Intelligent Transportation System (ITS) to be created by the deployment of autonomous and connected vehicle technology. A brief examination of the rationale for an intelligent system will be offered along with a general overview of the associated technologies. Insights into the similarities and distinct differences between the two technologies will also be outlined.

These new technology systems rely heavily upon the wireless transmission of data and communications and as a result, a high priority will be placed on securing networks from breach. Law enforcement officials can ill afford to limit cyber protections to just their information systems. Physical systems, such as police vehicle fleets operated nationwide have potential vulnerabilities that must be understood and protected from cyber attack. The thesis will highlight this problem area and discuss in detail a recent cybersecurity project undertaken by the Virginia State Police and the University of Virginia to address security of law enforcement fleet vehicles.

By virtue of the possible impacts on homeland security by the deployment of both technologies, law enforcement agencies, legislative bodies, judiciary members, and regulatory agencies across the country at all levels of government must be informed about this issue. Each entity will need to re-evaluate their operational, legislative, and regulatory processes in light of the complex changes wrought by an intelligent transportation system. These complex changes may affect statutory law, policy and agency response to incidents or events involving autonomous and connected vehicles.

It is believed that the thesis will serve as a law enforcement primer to educate Police Chiefs, Sheriffs, and State Police Superintendents across the nation on this emerging technology. The reader will be exposed to the technology and have a basic understanding of the principles of autonomous and connected vehicle technology, while simultaneously exploring the homeland security related issues of concern. Having a

---

[6] Mark Harris, "FBI Warns Driverless Cars Could Be Used as "Lethal Weapons,"" theGuardian.com, 2014, http://www.theguardian.com/technology/2014/jul/16/google-fbi-driverless-cars-leathal-weapons-autonomous.

fundamental understanding of the technology and system components is required of policy makers, law enforcement officials, and legislators in order that future regulation and policy decisions can be crafted effectively without stifling innovation.

A.   THE SURFACE HIGHWAY TRANSPORTATION SYSTEM

The surface highway transportation system impacts society in positive and negative ways. It encompasses "more than 250 million vehicles generating nearly 4 trillion passenger miles and 1.3 trillion motor carrier ton-miles annually on 4 million miles of roadway."[7] The functionality of the highway system directly affects the nation's economy as people depend on transportation for every facet of living the American dream.

From business to pleasure to accessing health care and other societal goals, vehicles are a staple of daily life. In 2012, the highway system supported the generation of 15,685 billion dollars in gross domestic product.[8] However, all of these opportunities are offset by large costs imposed on users. Connected vehicle technology is anticipated to lessen these costs through expedited traffic flow and better management of highway travel by consumers and management officials.[9] In metropolitan areas, time lost in traffic congestion results in lost productivity and wasted fuel consumption. For instance, a National Transportation statistic for 2011 indicated small urban areas with less than 500,000 populations resulted in 2.7 million gallons of wasted fuel.[10] Larger areas showed significant increases in waste, which ultimately result in increased demand for imported petroleum products.

---

[7] Transportation Research Board of the National Academies, *Critical Issues in Transportation 2013* (Washington, DC: Transportation Research Board of the National Academies, 2013), 4, http://onlinepubs. trb.org/Onlinepubs/general/criticalissues13.pdf.

[8] "Table 3–10: National Transportation and Economic Trends," accessed July 16, 2014, http://www. rita.dot.gov/bts/sites/rita.dot.gov.bts/files/publications/national_transportation_statistics/html/ table_03_10.html.

[9] AASHTO Executive Committee, *AASHTO Connected Vehicle Field Infrastructure Footprint Analysis: Preparing to Implement a Connected Vehicle Future: Preparing to Implement a Connected Vehicle Future* (Washington, DC: American Association of State Highway and Transportation Officials, 2014), http://stsmo.transportation.org/Documents/Executive%20Briefing.pdf.

[10] "Table 4–28: Annual Wasted Fuel Due to Congestion," accessed July 16, 2014, http://www.rita.dot. gov/bts/sites/rita.dot.gov.bts/files/publications/national_transportation_statistics/html/table_04_28.html.

The most telling statistic for review, however, is the deaths and injuries from crashes. In 2011, nationwide there were 5.6 million crashes resulting in 2.3 million injuries and 33,561 fatalities.[11] Virginia's statistics reveal 120,513 crashes resulting in 63,382 injuries and 764 fatalities for the identical period.[12] The resultant losses in property, social costs, and civil litigation easily reach into the billions.[13] It is this phenomena that safety advocates and law enforcement agencies across the nation attempt to address with a variety of regulations, enforcement and educational programs with limited success. It is believed that the use of autonomous technology which allows precise vehicle operation with limited to no input from a driver, and connected vehicle technology which provides situational awareness to drivers of the vehicle's operating environment can significantly reduce these alarming numbers.[14]

There are several barriers to be overcome before this technology can be fully implemented, but not all concern national security. For example, costs to the consumer may be initially exorbitant, and liability issues have yet to be addressed.[15] Additionally, the potential for violations of information privacy could be highlighted as vehicles transmit data wirelessly concerning the vehicle. Because these vehicles are connected to each other, infrastructure, and possibly the Internet it is the threat of cyber attacks on the connected systems the vehicles employ that is a national security concern.[16]

---

[11] "Table 2–17: Motor Vehicle Safety Data," accessed July 16, 2014, http://www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/publications/national_transportation_statistics/html/table_02_17.html.

[12] "2011 Virginia Crash Facts," accessed July 24, 2014, www.dmv.state.va.us/safety/crash_facts/crash_facts_11.pdf.

[13] "New NHTSA Study Shows Motor Vehicle Crashes Have $871 Billion Economic and Societal Impact on U.S. Citizens," accessed July 24, 2014, http://www.nhtsa.gov/About+NHTSA/Press+Releases/2014/NHTSA-study-shows-vehicle-crashes-have-$871-billion-impact-on-U.S.-economy,-society.

[14] "U.S. Department of Transportation Releases Policy on Automated Vehicle Development," May 30, 2013, http://www.nhtsa.gov/About+NHTSA/Press+Releases/U.S.+Department+of+Transportation+Releases+Policy+on+Automated+Vehicle+Development.

[15] "How Autonomous Vehicles Will Shape the Future of Surface Transportation," accessed July 6, 2014, http://transport.house.gov/calendar/eventsingle.aspx?EventID=357149.

[16] Kristin M. Finklea and Catherine A. Theohary, *Cybercrime: Conceptual Issues for Congress and US Law Enforcement* (CRS Report No. R42547) (Washington, DC: Congressional Research Service, 2012), http://mercury.ethz.ch/serviceengine/Files/ISN/146602/ipublicationdocument_singledocument/653ce4be-1832-448a-a09c-bbebd7d2b08c/en/193706.pdf.

There are two related, yet separate technology concepts that require brief discussion. The two technologies, autonomy, and connectivity are being independently developed and can function independent of one another. It is anticipated that at some point in the future a merger will occur as both systems become robust and gain user acceptance. Both systems will be covered in the following chapters at a macro level to facilitate a basic understanding of how the technologies will function.

Autonomous vehicles do not require connected vehicle technology to operate, however overall safety is improved due to sensing information being received from other vehicles and infrastructure.[17] Autonomous vehicle technology touts the same benefits as connected vehicles, but also includes the capability for drivers to be relieved of some, if not all, responsibility for input in the actual operation of a vehicle while in motion. By using complex computer algorithms and optical sensors, the vehicles are able to become autonomous with limited or no action necessary for drivers.[18] The word driver may instead be replaced by user at the highest level of automation, requiring changes to existing legal definitions for that term. Autonomous vehicle technologies are essentially driver assistance systems that perform functions, such as navigating the vehicle through specific traffic situations for example lane changes, cruising at speed, parking and turning.

Connected vehicle technology consists of sensors on board the vehicle, as well as embedded in infrastructure that communicate position, speed, and direction of travel to vehicles in proximity.[19] Creating greater driver awareness of traffic conditions should lead to a reduction in traffic accidents and property loss.

The equipment used by both connected and autonomous vehicles provide the vehicle with a 360-degree view/sense of its surroundings while allowing it to communicate and receive signals/data from infrastructure and other vehicles. The two

---

[17] James M. Anderson et al., *Autonomous Vehicle Technology: A Guide for Policymakers* (Santa Monica, CA: RAND Corporation, 2014), http://www.rand.org/pubs/research_reports/RR443-1.html.

[18] Ibid., 8–65.

[19] AASHTO Executive Committee, *AASHTO Connected Vehicle Field Infrastructure Footprint Analysis: Preparing to Implement a Connected Vehicle Future*.

technologies will operate simultaneously to achieve the greatest value in autonomy; however, it is the wireless transmission characteristic that exposes these vehicles to possible cyber intrusion.

B.   RESEARCH QUESTION

The topic was selected because of the wide-ranging impact it will have on law enforcement and homeland security. This technology if determined to be safe and accepted by the general public has the potential to fundamentally reshape transportation worldwide. This thesis answers the question, what are the likely and emerging law enforcement policies, regulatory, and system security issues surrounding autonomous and connected vehicles?

Law enforcement, legislators, and judicial officials responsible for highway safety must be made aware of what specifically this technology will do and the resultant changes that will be required when upper levels of autonomy are reached. It is hoped that this thesis will serve as a law enforcement primer on the subject of autonomous and connected vehicles with heavy emphasis on securing the systems from bad actors to minimize/prevent misuse by cyber attack. Limited articles have been written on this topic from a Homeland Security perspective and it is hoped this thesis will begin to fill that void.

The technology is rapidly expanding and detailed studies by academics, government agencies and private corporations are underway with emphasis on making both autonomy and connectivity function safely and correctly. In order to gain user acceptance and ensure successful deployment both systems must prove their value to the consumer.

C.   SCOPE AND LIMITATIONS

While a generalized description of autonomous and connected vehicle functions will be required it is not the intent of this thesis to discuss the technical specifications of how these vehicles are programmed to operate under any given condition. Technical and computerized functions while related are not central to this inquiry and will not be

described. It will be assumed that systems function as designed, but discussion about how those systems might be compromised will be undertaken with a view to minimize the impacts to law enforcement and homeland security.

It will not be possible to describe what the final communications security system will look like or what entity will provide that service. The thesis will also not address how autonomous functions might be deployed and used by law enforcement and other public safety officials to enhance public safety service delivery.

D.   SOURCES AND METHODS

The sources of data for this work come exclusively from examination of existing and emerging literature to include journal articles and technical papers, government documents, and private industry articles.

The U.S. Department of Transportation (USDOT) maintains responsibility for management of highway systems to ensure national interests are met.[20] This organization will ultimately oversee the implementation of autonomous and connected functions in vehicles. The research, standards, directives, and federal laws generated by USDOT will be used as written sources to define and outline concepts of technology and regulation of this technology.

As this topic involves an emerging technology, the methodology will reside fully within the Hypothetical - Theoretical realm. The mode of analysis used will be Predictive and entirely based on forecasting. The described systems have not been fully defined and performance criteria are not subject to evaluation. Conclusions and recommendations can be offered based on existing data and proposed system design.

E.   CHAPTER OVERVIEW

A macro-level view of the technologies involved with autonomous vehicles that make them function will be undertaken in Chapter II. It is important that policy makers have a basic understanding of what the technology is and how it functions. This

---

[20] "About DOT," accessed November 2, 2015, http://www.transportation.gov/about.

knowledge will benefit leaders who may need to make organizational or policy changes as a result of this emerging technology.

Chapter III will focus on connected vehicle technology and how communications between vehicles, the infrastructure, and personal communication devices are projected to work. Ensuring the security of the connected vehicle systems from penetration by bad actors will be an enormous task and vital to public acceptance of this technology. How these security systems will be developed, operated, and regulated is currently under study by the Department of Transportation, academics, and other private stakeholders. What form the communication systems will take has yet to be decided and might include a government controlled system, private system, or hybrid public-private partnership.

As these systems emerge on the market, they will have a measurable impact on society. An examination of potential positive and negative societal impacts deriving from the introduction of the technology will be discussed in Chapter IV. Sometimes new technologies create unintended consequences and the potential for this technology to be disruptive will also merit discussion. Homeland Security will be directly impacted as this technology could be used for a multitude of nefarious purposes to advance criminal enterprises. Some examples discussed will include aiding in the furtherance of crimes like drug trafficking, kidnapping, insurance fraud, or even the potential for this technology to be used as a mechanism for creating vehicle borne explosive devices.

Cybersecurity related issues have significantly increased in size, scope, and financial impact. However, most media coverage surrounding this area is related to cyber attacks on information systems. It is logical to suggest that future cyber attacks may also be directed at physical systems like automobiles. In particular, the ability to launch attacks against public safety vehicles is of significant concern and should warrant serious analysis.

Chapter V highlights this issue and in particular outlines a cybersecurity public-private partnership involving the Virginia State Police, and the University of Virginia, the MITRE Corporation, the Aerospace Corporation, and several private cybersecurity firms undertaken to examine cyber vulnerabilities in state police vehicles. The project also

received coordination from the U.S. Department of Transportation Volpe National Transportation Training Center and the U.S. Department of Homeland Security Science and Technology Directorate.

This cybersecurity project was performed on modern police vehicles and not connected or autonomous vehicles. However, the same systems on the current vehicles will be the focus of hackers as the new technology is unveiled. Protecting the data transmissions that occur throughout the vehicle will be of utmost importance going forward. Modern-day vehicles contain multiple computers that relay information through a controller area network (CAN) bus. The CAN bus is connected to almost all critical systems in the vehicle and once hackers have gained access to it, they can manipulate various vehicle systems by understanding the data codes that are transmitted by the bus.

The fifth chapter will outline the phases of the study and reveal the findings and offer recommendations for policy makers to consider. Protection and mitigation strategies will be offered as well so that agency heads can prepare now to ensure the integrity of their police vehicle fleets.

The final chapter will serve as a conclusion and offer further recommendations for consideration as autonomous and connected vehicle technology enters the market place. This technology has the capacity to be disruptive; serious study of its impact on homeland security from a variety of perspectives should not be ignored. Public safety officials are encouraged to evaluate every operational, regulatory, and legislative process currently being undertaken with an eye towards implementation in the next decade of this technology.

THIS PAGE INTENTIONALLY LEFT BLANK

II. AUTONOMOUS VEHICLE TECHNOLOGY

The idea of autonomy in vehicles is not a new concept. The 1939 World's Fair in New York contained an exhibit by General Motors entitled Futurama.[21] It provided fair goers a glimpse of how every facet of daily life would be transformed by automation in the year 1960. The video predicted that vehicles would travel along express motorways with seven lanes at speeds of 50, 75, and 100 miles per hour.[22] Highways in that depicted future were engineered for speed and safety and somewhat resemble current day interstate systems. The cars maintained appropriate following distances by use of radio signals.[23] Reliance on technology to improve safety and envisioning new horizons was the theme and that vision of autonomy for motor vehicles is nearing implementation in America today.

Most major car manufacturers and some transportation related private corporations have active research and development programs related to autonomous vehicles underway. While the specific corporations have slightly different goals in mind for autonomous functions in their respective products, the overarching concept is for the driver, at times, to be relieved of responsibility for the driving function. Technology will assume the role of operator while the human subject is removed from the equation. This transitional activity of going from human driver to machine driver and back to human is complicated and will require sound cognitive abilities matched with a friendly interface to allow the process to function without jeopardizing safety.

This chapter will illustrate how autonomous technology is anticipated to work. Individual components of the collective system will be discussed to provide background. It is important for homeland security practitioners to understand the basic concept behind vehicle automation in order to evaluate current law enforcement and security practices

---

[21] Anderson et al., *Autonomous Vehicle Technology: A Guide for Policymakers*, 1.

[22] "Futurama 1939 New York World's Fair 'To New Horizons' 1940 General Motors 23min," YouTube video, posted by Jeff Quitney, August 7, 2012, https://www.youtube.com/watch?v=1cRoaPLvQx0.

[23] Ibid.

that will be impacted as autonomous vehicles enter the consumer market. Additionally, a brief discussion of driver assistance systems, which are the precursors to autonomy, will be discussed by looking at examples from automakers, and private corporations. These systems are currently available on the consumer market in many product lines and are not limited to high-end models.

Lastly, the Technology Acceptance Model by Fred Davis will be applied to autonomous vehicle technology to provide an understanding of how likely it will be for consumers to actually use the technology. Law enforcement officials will be responding to incidents involving this technology and a fundamental understanding of autonomous systems will ensure agencies are prepared to handle those incidents.

A.   AUTONOMOUS VEHICLE TECHNOLOGY

The components necessary for an autonomous vehicle to function are varied depending on the desired level of automation required, but a general list would include the following:[24]

- Lidar—light detection and ranging

- Radar—radio detection and ranging

- Global positioning systems (GPS)

- Cameras

- Optical sensors

- On-board computer

---

[24] "Future Cars: The Word from GM at IDC's Smart Technology World Conference|Steve Leibson," accessed September 2, 2015, http://low-powerdesign.com/sleibson/2011/05/01/future-cars-the-word-from-gm-at-idc%E2%80%99s-smart-technology-world-conference/.

Figure 1.   Future Cars: The Word from GM at IDC's Smart Technology
World Conference
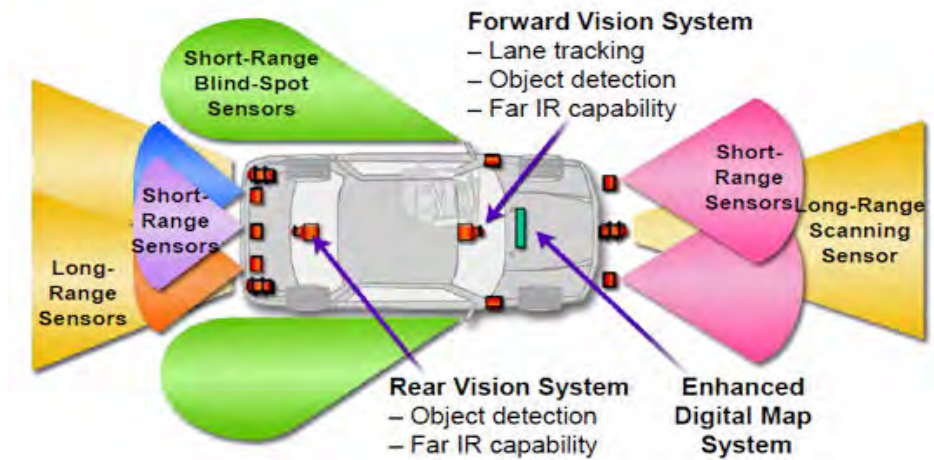
B.   LIDAR

Laser based sensing technology began in the 1970s by the National Aeronautics and Space Administration (NASA) for space borne deployment.[25] During the middle of the next decade, experimentation at Stuttgart University validated the use of lidar as a highly accurate method for topographic mapping.[26] By the mid-1990s, laser-based systems were being manufactured capable of delivering sensors with the capacity to emit 25,000 pulses per second. The returns from the pulses were used to map features of topography with high accuracy. Today, over 200 lidar systems are operational worldwide with the capacity to emit 250,000 pulses per second.[27]

Today's technological advances increase exponentially. Lidar systems create highly detailed three dimensional models used by the vehicle's on-board computer for

---

[25] "History of Lidar Development|GEOG 481: LIDAR Technology and Applications," accessed July 10, 2015, https://www.e-education.psu.edu/geog481/l1_p4.html.

[26] Ibid.

[27] Ibid.

path planning.[28] By preloading maps of traffic infrastructure, stationary items like signage, traffic lights, and crosswalks are known. The lidar light measurements reveal the moving objects like people and other moving traffic.

The Lidar unit is central to the function of autonomy in motor vehicles. Also known as a laser range finder this unit measures distances between objects and the vehicle by emitting pulses of light while spinning on its axis and modifying the pitch.[29] The system is comparable to radar but uses light as opposed to radio waves.

One such system, manufactured by Velodyne Inc., uses sixty-four separate lasers that are mounted at various pitch angles.[30] This system is highly visible on the roof of early Google car fleet vehicles and consists of the rotating lidar, which allows the lasers to scan the entire environment surrounding the vehicle, producing a three dimensional map.[31] The highly detailed map is constantly updated as the Lidar takes millions of measurements per second.[32] The relative motion of the vehicle allows moving objects to be identified and tracked with precision.[33]

The system is not without limiting factors. The long-range lidars used in autonomous vehicles have a relatively short range of approximately 120 to 150 meters (393–492 feet) with a thirty-degree horizontal and vertical view.[34] While shorter-range lidars 50 to 80 meters (164–262 feet) provide thirty degrees of vertical scan and a 360-degree horizontal view.[35] In addition, poor reflection from certain kinds of materials can impact imagery.[36]

---

[28] "History of Lidar Development|GEOG 481: LIDAR Technology and Applications," 58–65.

[29] "Google Driverless Car—The Obstacle Detection Unit," June 14, 2014, http://www.whatafuture. com/2014/06/14/google-driverless-car-the-obstacle-detection-unit/.

[30] Ibid.

[31] Iain David Graham Macdonald, *A Simulated Autonomous Car* (Edinburgh: The University of Edinburgh, 2011), 10, http://www.inf.ed.ac.uk/publications/thesis/online/IM110982.pdf.

[32] Anderson et al., *Autonomous Vehicle Technology: A Guide for Policymakers*, 61.

[33] "Google Driverless Car—The Obstacle Detection Unit."

[34] Brian Cullinane et al., "Engaging and Disengaging for Autonomous Vehicles," US9075413 B2, filed July 17, 2014, and issued July 7, 2015, 4, http://www.google.com/patents/US9075413.

[35] Ibid.

[36] Anderson et al., *Autonomous Vehicle Technology: A Guide for Policymakers*, 62.

Figure 2.   Sensing System Components and Effective Ranges
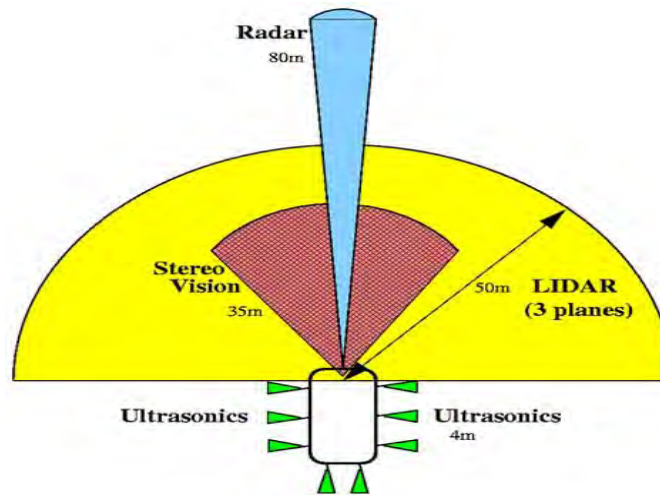
Source: Umit Ozguner, Christoph Stiller, and Keith Redmill, "Systems for Safety and Autonomous Behavior in Cars: The DARPA Grand Challenge Experience," *Proceedings of the IEEE* 95, no. 2 (2007): 397–412.

C.   RADAR

The development of radio detection and ranging has its origins in the United States Navy. Prior to radar deployment Navy ships could track other vessels by use of optics or sound ranging or primitive radio direction finding. Naval researchers soon developed a process for using radio waves to identify moving vessels.[37] This radar principle was later refined during the 1930s to include radio detection and ranging. The system proved invaluable during World War II and contributed to numerous naval victories.

Autonomous vehicles will rely on radar units mounted on the front and rear of the vehicle, as well as the front and rear bumper.[38] The units emit radio waves and measure the change in frequency of the return waves to provide range to objects in the vehicle's environment.[39] These devices are also used to support driver assistance systems like adaptive cruise control, which when activated automatically adjusts the speed of a vehicle

---

[37] "Development of the Radar Principle," accessed July 10, 2015, http://www.nrl.navy.mil/accomplishments/systems/radar/.

[38] "Google Driverless Car—The Obstacle Detection Unit," 3.

[39] Anderson et al., *Autonomous Vehicle Technology: A Guide for Policymakers*, 62.

relative to the speed of the vehicle it is following. These units typically have a range of 60 to 200 meters (196 to 656 feet), and an associated beam width of 18 degrees to 56 degrees.[40]

D.   GLOBAL POSITIONING SYSTEMS

Global positioning systems (GPS) originated during the Vietnam War era to aid the military, and were later made available for civilian use almost a decade and a half later.[41] The U.S. Air Force ensures that at least 24 of 31 satellites are available at all times for operational use.[42] The system transmits radio frequency signals, which are captured by ground base receivers to provide location, speed, and time information to users using a method called trilateration.[43]

Most new vehicles come equipped with an on-board navigation system using GPS technology, and mobile units are available to consumers as add on equipment to older model vehicles. Portable electronic devices, such as cellular phones and tablets offer similar services.

GPS receivers usually track four to seven satellites at a time and couple the triangulated data with previously stored road map, and topographical data to display information in a user-friendly format.[44]

The GPS system provides free real time data in all weather conditions, and is available globally on a 24-hour-a-day basis. Since the U.S. military developed the system, some thought was given to how the system could be potentially used by adversaries against the United States. The receivers used to triangulate position are generally accurate to within 15 meters (49 feet) and newer models utilizing wide area

---

[40] Cullinane et al., "Engaging and Disengaging for Autonomous Vehicles," 4.

[41] Wan Rahiman and Zafariq Zainal, "An Overview of Development GPS Navigation for Autonomous Car," in *2013 IEEE 8th Conference on Industrial Electronics and Applications (ICIEA)* (2013), 1112, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6566533.

[42] "'How GPS Works' Poster," accessed June 8, 2015, http://www.gps.gov/multimedia/poster/.

[43] "How Does GPS Work?," December 16, 2014, 2, http://gps.about.com/od/beforeyoubuy/a/how gpsworks.htm.

[44] Ibid., 3.

augmentation system signals can narrow that margin of accuracy closer to three meters (nine feet).[45] The military designers opted to degrade the systems accuracy by applying small errors in timing and satellite position. This decrease in accuracy, generally around 100 meters (328 feet) is referred to as selective availability.[46]

While GPS systems provide accurate location information that autonomous vehicles will rely on the system is not foolproof. The signals are transmitted via microwaves, which can be absorbed by water resulting in reception problems during periods of inclement weather. Additionally, line of sight to multiple satellites is required for functionality so heavy foliage and tall structures in an urban environment could hinder reception as well.[47]

Another important consideration critical to autonomy is that GPS data alone does not provide vehicle orientation or speed estimation. The GPS unit must work in concert with an inertial measurement unit containing a gyroscope and accelerometer to estimate velocity and acceleration of the vehicle.[48] Modern day commercial systems available to the general public contain all of these elements in single units that can be purchased at reasonable cost.[49]

E.   CAMERAS

A variety of cameras may be mounted on the vehicle to validate and provide distance measurements to objects detected by the sensor network.[50] The system may be equipped with still cameras or video cameras to capture images of the environment. These images would be compared with stored data in the on-board computer system to facilitate path planning and object detection. The range that these units will scan an area

---

[45] "How Does GPS Work?," 4.

[46] Johann Borenstein et al., "Mobile Robot Positioning-Sensors and Techniques," DTIC, 1997, 11, http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA422844.

[47] Ibid., 13.

[48] Gregory Dudek and Michael Jenkin, "Inertial Sensors, GPS, and Odometry," in *Springer Handbook of Robotics* (Berlin: Springer, 2008), 484–489, http://link.springer.com/10.1007/978-3-540-30301-5_21.

[49] Rahiman and Zainal, "An Overview of Development GPS Navigation for Autonomous Car," 1112.

[50] Cullinane et al., "Engaging and Disengaging for Autonomous Vehicles," 4.

is typically between 100 and 200 meters (328 to 656 feet) in front of the vehicle with horizontal coverage between 30 to 60 degrees.[51]

F. OPTICAL SENSORS

There are a variety of sensors currently housed within motor vehicles that provide indications of system performance and functionality. Vehicle manufacturers currently install sensors that provide information on tire pressure, engine temperature, oil level and other system critical functions.[52] Additional sensors are required for autonomous and connected vehicles to operate efficiently and will require real time updating of the environment external to the vehicle.[53] This sensing of data will be compared to existing environmental data (stored mapping software) to allow for path planning and execution of vehicle maneuvers.

Sensing devices may be mounted at various levels around the vehicle to provide 360-degree horizontal and vertical coverage. These laser rangefinders are mounted at various heights to allow for horizontal estimations of object height as the vehicle approaches an obstacle.[54] Vertical scanning provides details of the ground profile ahead of the vehicle. Ultrasonic rangefinders mounted on the sides of vehicles will provide side sensing and rear sensing capability.[55]

G. ON-BOARD COMPUTER

The on-board computer system must be of sufficient computational strength to handle complex computing of all data received from the sensor network. Configurations are not standardized and will vary across the range of manufactured automobiles. The computer systems in autonomous vehicles will execute complex computer algorithms to operate safely in autonomous mode based on sensor data and programming software.

---

[51] Cullinane et al., "Engaging and Disengaging for Autonomous Vehicles," 4.

[52] "All about Sensors|A Guide to the Use, Applications, and Technology of Sensors," accessed September 29, 2015, http://www.sensorsweb.com/temperature_sensors.

[53] Ozguner, Stiller, and Redmill, "Systems for Safety and Autonomous Behavior in Cars: The DARPA Grand Challenge Experience," 398–399.

[54] Ibid., 403.

[55] Ibid.

Some systems may require initial input from the user through direct action or voice activated command to engage the system.[56]

The computer network will also include all electronic control modules currently installed within standard vehicle electrical systems to allow for monitoring of vehicle components and operations. A fail-safe mechanism will be incorporated into the design to maximize safety in the event of system failure.

Also included in the programming software will be methodology for handing off the autonomous function to a human operator and returning the vehicle to autonomous operation from the human driver. Known as the human / machine interface (HMI) this transitional activity is currently under intensive study by numerous universities and transportation institutes.[57] Ensuring smooth transition between the operator and the vehicle is critical for safety and gaining user acceptance.

Challenges with HMI include what impact transfer will have on a drivers' cognitive ability to process information and how potential increases in level of workload during transfer operations will impact safety.[58] Should drivers misunderstand, misuse or otherwise become complacent as a result of overconfidence in automated features then common driving tasks could have dangerous consequences.[59]

The previous descriptions are not all inclusive and may vary across manufacturers. Newer more robust technology should emerge as research and development continue. There are precursors of autonomy currently available on a number of automobiles and that are being marketed as driver assistance systems. A sampling of these systems from automakers, suppliers, and private corporations will now be discussed.

---

[56] Dmitri Dolgov et al., Systems and Methods for Transitioning Control of an Autonomous Vehicle to a Driver, US20140303827 A1, filed April 5, 2013, and issued October 9, 2014, 1, http://www.google.com/patents/US20140303827.

[57] Tammy E. Trimble et al., *Human Factors Evaluation of Level 2 and Level 3 Automated Driving Concepts: Past Research, State of Automation Technology, and Emerging System Concepts* (Blacksburg, VA: Virginia Tech Transportation Institute, 2014).

[58] Ibid., 2.

[59] Ibid., 1

H.   DRIVER ASSISTANCE SYSTEMS

There have been many examples of successful testing of autonomous functions by original equipment manufacturers (OEMs).[60] Many of the major car manufacturers have autonomous vehicle divisions within their organizations, and are advancing the use of driver assistance systems, which are the preliminary steps in autonomy. It is envisioned that the driver assistance systems will lead to increased autonomous functionality in incremental steps over the next decade.[61]

The BMW Group announced an ambitious business model by projecting self-driving vehicles in the year 2020.[62] The current inventory of vehicles offers traffic jam assist and parking assist in various vehicle models.[63] Traffic jam assistant can be used by drivers during high congestion, slow movement situations by regulating speed even to a full stop. Lane keeping functions can also be activated if contact is maintained with the steering wheel.[64]

BMW vehicles also are equipped with parking assist features that identify available parking spaces if certain parameters are maintained. The system will select the appropriate gear (forward or reverse) and will automatically steer into the space while adjusting braking and acceleration as needed.[65] Optical and ultrasonic sensors allow the technology to work as data flows to the central computer and then to actuators that manipulate steering, braking, and acceleration functions while providing situational awareness to the driver.

---

[60] Ozguner, Stiller, and Redmill, "Systems for Safety and Autonomous Behavior in Cars," 399.

[61] "Countdown to Mainstreaming of Self-Driving Vehicles accessed July 11, 2014, https://www.enotrans.org/eno-brief/countdown-to-mainstreaming-of-self-driving-vehicles."

[62] Stephen Elmer, "BMW Targets 2020 for Self-Driving Cars," *Auto Guide*, February 26, 2013, http://www.autoguide.com/auto-news/2013/02/bmw-targets-2020-for-self-driving-cars.html.

[63] "BMW X5 : Driver Assistance," accessed July 14, 2015, http://www.bmw.com/com/en/newvehicles/=x/x5/2013/showroom/driver_assistance/index.html.

[64] Ibid.

[65] Ibid.

Figure 3.   Driver Assistance Systems: Product Design and Development
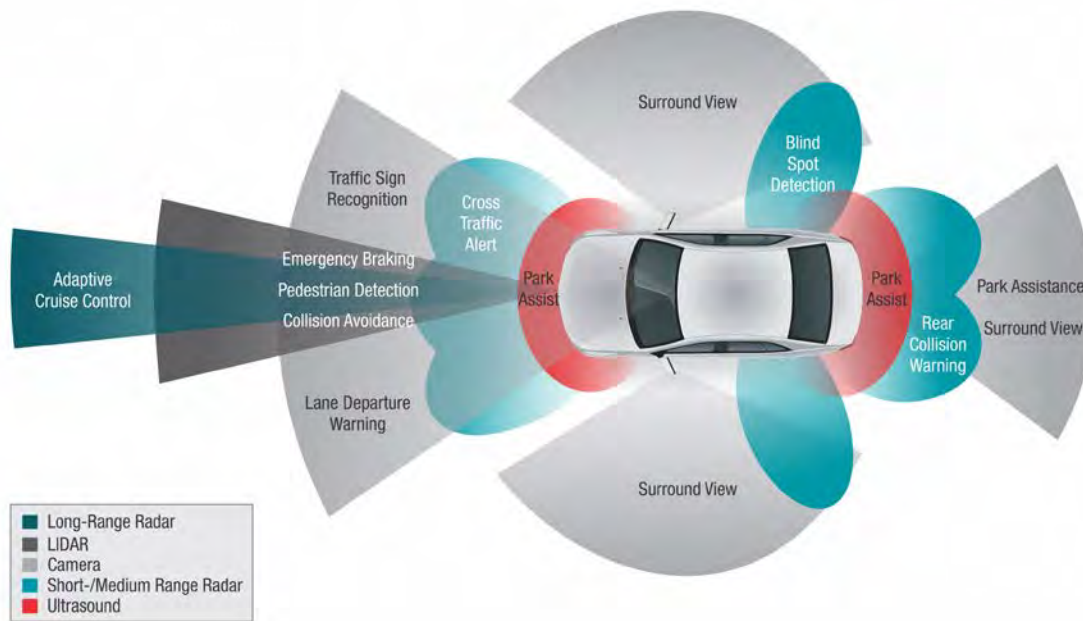
Source: "Updated: Advanced Driver Assistance Paves the Way for Autonomous Car," *Product Design and Development*, accessed September 2, 2015, http://www.pddnet. com/article/2013/11/updated-advanced-driver-assistance-paves-way-autonomous-car.

In October 2014, to illustrate that autonomous functions in vehicles are not limited to low speeds, an Audi RS7 Piloted Driving Concept vehicle successfully lapped the Hockenheimring racetrack in Germany at high speeds (140 mph), using only computers and sensors to guide it.[66] The vehicle successfully maneuvered around the track negotiating left and right hand turns with ease. While this level of speed and precision is not the norm for most manufacturers at this stage of development, the test does illustrate control and safety in a high-speed environment, which serves to foster user acceptance of the technology.

A more nuanced approach to active testing of the technology was undertaken by Delphi, a tier one automotive supplier in March 2015, when the company set out on a cross-country journey of 3,400 miles. The team of engineers and the vehicle called

---

[66] Peter Valdes-Dapena, "Audi Driverless Car Hits 140 Mph," *CNNMoney*, October 17, 2014, http:// money.cnn.com/2014/10/17/autos/audi-rs7-driverless-racetrack/index.html.

Roadrunner made the longest autonomous road test documented to date.[67] The on-board equipment reportedly performed flawlessly.[68]

Google's autonomous vehicle-testing program in California has accumulated in excess of 1,000,000 miles.[69] With a fleet of twenty vehicles and fifty test personnel the software giant continues to develop the software that will be offered to consumers that will facilitate autonomy in vehicles. A special fleet of vehicles has also been created without steering wheels and pedals, which has drawn the attention of NHTSA.[70]

The Google vehicle's central computer responds to the algorithms designed by the software engineers that tell the car what to do under various driving situations that it might face, from identification of roadway markings and signage to what to do should it detect that the driver has become incapacitated.[71]

Google anticipates linking user accounts to the driverless car.[72] Data related to users profiles will be stored and maintained on the vehicle's computer. By logging into the system, and verifying identity, users can define specific protocols to be followed.[73] For example, limiting the maximum speed of a vehicle used by a juvenile, restricting location where the vehicle can be taken, and maintaining a log for inspection by owners or fleet managers.[74] These controls will provide margins of safety, which are programmable and will help establish user acceptance that the vehicle will not be used for purposes outside the owner's pre-established limits.

---

[67] "Delphi Drive."

[68] Ibid.

[69] Isidore, "Injuries in Google Self-Driving Car Accident."

[70] David Shepardson, "U.S. Urges Google to Focus on Safety in Driverless Test," *Detroit News*, January 21, 2015, http://www.detroitnews.com/story/business/autos/2015/01/21/google-safety-driverless-test/22116531/.

[71] "Google Driverless Car—Data Stored in the Car Memory," June 26, 2014, http://www.whatafuture.com/2014/06/26/google-driverless-car-data-stored-in-car-memory/.

[72] Ibid.

[73] Ibid.

[74] "Google Driverless Car: Limiting Destination Abilities Will Prevent Its Misuse," May 27, 2014, http://www.whatafuture.com/2014/05/27/google-driverless-car-your-car-will-prevent-its-own-misuse/.

To date the fleet of Google vehicles comprised of 23 Lexus RX450 Hybrid and 25 compact prototype cars have been involved in several accidents.[75] The most recent resulted in injury after the autonomous vehicle was rear-ended at an intersection.[76] The vehicles have accumulated over one million miles in self-driving mode and are operated about 10,000 miles per month.[77] According to Google executives, none of the accidents have occurred as a result of the autonomous function.[78]

While auto safety is promoted as the desired outcome, the technology will broaden the scope of users to include individuals with mobility challenges, and those too young to be licensed.[79] Additionally, senior citizens with diminished driving skills will maintain access to mobility.[80] A natural by product for all persons over time will then be the erosion of driving skills.

These increased numbers of vehicles will negate the overall benefit of decreased congestion through increased demand and use of petroleum products and other implied costs, such as increased potential for accidents and related liability costs.[81] According to the Federal Highway Administration in 2011, there were 210 million licensed drivers in the United States.[82] In a U.S. News and World report, the U. S. Census Bureau estimate of the nation's population for the same period was 310.5 million people, or approximately a 67 percent increase in the number of potential users of transportation.[83]

---

[75] Isidore, "Injuries in Google Self-Driving Car Accident."

[76] Ibid.

[77] Ibid.

[78] Ibid.

[79] David Levinson, "Climbing Mount Next: The Effects of Autonomous Vehicles on Society," *Minn. JL Sci. & Tech.* 16 (2015): 787–1011.

[80] Ibid.

[81] Bryant Smith, "Managing Autonomous Transportation Demand," *Santa Clara Law Review* 52, no. 4 (December 19, 2012): 1401.

[82] "Office of Highway Policy Information (OHPI)—Highway Finance Data Collection," accessed July 29, 2014, https://www.fhwa.dot.gov/policyinformation/pubs/hf/pl11028/.

[83] Robert Schlesinger, "U.S. Population, 2011: 310 Million and Growing," *US News & World Report*, December 30, 2010, http://www.usnews.com/opinion/blogs/robert-schlesinger/2010/12/30/us-population-2011-310-million-and-growing.

An increase in vehicle miles traveled, which is the number of miles traveled in a year by motor vehicles of all types on public roads and streets of all types, will occur as more users take advantage of reduced costs and autonomy.[84] As autonomy becomes accepted commuting distances are expected to increase. Responsibility for driving will have been removed from the user, who can now be more productive during the travel period thus potentially increasing urban sprawl.

Autonomy is expected to provide societal benefit in the form of reduced injuries and death from crashes, and positive change in environmental conditions.[85] Before those results can be achieved however, the technology must be accepted by the end user as safe and reliable. To gain insight into technology acceptance a brief examination of a useful model will be undertaken.

I.   TECHNOLOGY ACCEPTANCE MODEL

The introduction of new technologies into the marketplace can have mixed results. As this particular technology could directly impact individual safety it may take some time before consumer acceptance grows as illustrated by the Technology Acceptance Model introduced by Fred Davis in 1989.

Figure 4.   Technology Acceptance Model
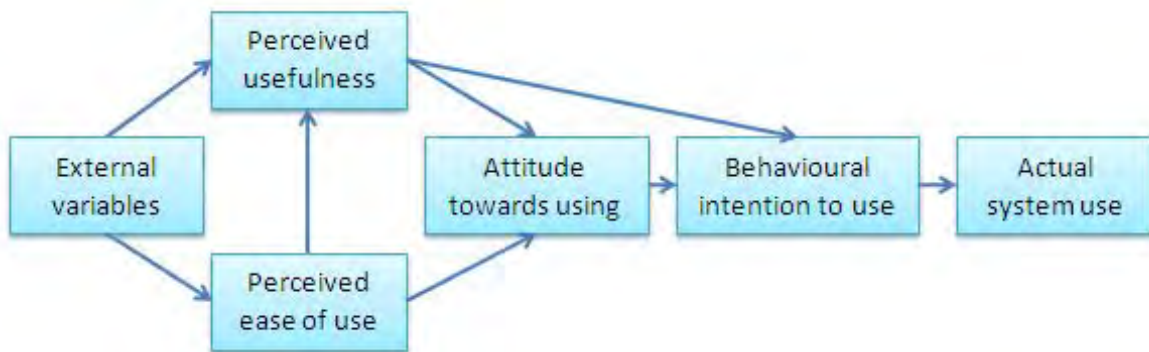
Source: Fred Davis, Richard Bagozzi, and Paul Warshaw, "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models," *Management Science* 35, no. 8 (August 1989): 22.

---

[84] Smith, "Managing Autonomous Transportation Demand."

[85] Levinson, "Climbing Mount Next: The Effects of Autonomous Vehicles on Society," 787–1011.

The model suggests that the intention to accept and then use new technology revolves around two key factors:

- Perceived Usefulness of the technology

- Perceived Ease of Use of the technology[86]

The perceived usefulness of autonomous vehicle technology can be considered as the degree to which an individual thinks the self-driving systems will improve their performance or quality of life. While the perceived ease of use relates to how effortlessly the technology can be activated and de-activated by the individual to satisfy daily driving requirements.[87]

Davis theorized that increases in usefulness and ease of use correlates to an increased level of positive attitude toward using the technology.[88] If manufacturers can create a system that is simple, yet efficient to control complex driving behaviors and demonstrate an acceptable level of safety then users will begin to accept it. Further, the elevated attitude correlates directly to the behavioral intention to use the technology, and ultimately actual use of an autonomous system.[89]

Other factors (variables), also impact the usefulness and ease of use considerations. These factors could be simply general observations and impressions (safety) from other individuals about the technology. Bias in perceptions of product manufacturing processes could play a role in accepting certain vehicle makes and models. Cultural bias about socioeconomic status could likewise affect the behavioral intention to use the technology.

The unknown variable that could affect user acceptance on a large scale could be the implied safety benefits to be derived. One crucial element of that safety factor is an

---

[86] Levinson, "Climbing Mount Next: The Effects of Autonomous Vehicles on Society," 985.

[87] Ibid.

[88] Ibid.

[89] Ibid.

effective communications system that transmits the data to all users. It must provide a viable, safe, low latency, and secure platform.[90]

Davis' model also suggests that when analyzing the two main factors, one plays a stronger role in the behavioral intent to use.[91] The perceived usefulness of a self-driving vehicle will have a greater impact on the individual than the ease of use. One could certainly argue that a self-driving vehicle offers extreme usefulness in addition to simplicity in use. But if the technology cannot prove itself to be better than the average human driver there will not be much of an incentive to use it.

J.   CONCLUSION

Autonomous vehicles have the potential to positively affect safety, decrease congestion, energy consumption and offer viable alternatives for transportation to those with mobility challenges, such as the physically disabled and senior citizens.[92] It is important to remember that the equipment installed on a vehicle to make it autonomous does not create uniformity in terms of performance capability for all vehicles. Engine sizes and performance expectations will still vary among manufactured brands. This variance in performance sometimes creates conflicts in the safe movement of motor vehicles on the highway. Autonomous vehicle technology can lead to a safer environment as vehicles will detect and adjust driving maneuvers based on the data received from other vehicles in close proximity.

A separate but related technology currently under development is known as connected vehicle technology. This system provides driver awareness of safety critical information and will enhance autonomy when the two technologies are coupled.[93] The technology does not have a direct effect on vehicle operation but merely provides

---

[90] "DSRC: The Future of Safer Driving Fact Sheet," accessed December 31, 2014, http://www.its.dot. gov/factsheets/dsrc_factsheet.htm.

[91] Davis, Bagozzi, and Warshaw, "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models," 986.

[92] "Lloyds Insurance Report: Overcoming Obstacles for Driverless Cars," accessed September 2, 2014, http://robohub.org/lloyds-insurance-report-overcoming-obstacles-for-driverless-cars/.

[93] NHTSA, *Planning for the Future of Transportation: Connected Vehicles and ITS.*

situational awareness to the driver that can allow for effective decision making while in transit. Understanding the connected vehicle technology system will be the subject of the following chapter.

THIS PAGE INTENTIONALLY LEFT BLANK

III.   CONNECTED VEHICLE TECHNOLOGY

The U.S. Department of Transportation's (USDOT) Intelligent Transportation Systems (ITS) ITS Strategic Plan 2015–2019 was released in December 2014.[94] This planning document is a continuation of the 2010–2014 strategic plan and outlines, in part a vision for connected vehicle (CV) technology and the path towards implementation.[95]

This chapter will identify key concepts associated with CV technology including discussion regarding the benefits to be derived from its use and the vision outlined for implementation. Key stakeholders will be identified along with their associated roles in development. A brief overview of key terms and concepts will clarify the lexicon used by stakeholders and give understanding to the relationships between organizations.

The current state of CV will be outlined for the reader and will include a generalized description of the various communications systems being considered to make the system function. Ensuring the integrity of the communications system will be critical to gain user acceptance. A public key infrastructure (PKI) program is currently under consideration as a methodology for security. A brief explanation of terms and modeling will be described as a final structure has yet to be realized and is currently under study.[96]

A general overview of putting CV theory into practice in real world scenarios is warranted and will be demonstrated by evaluating current test bed projects within the United States in Michigan and Virginia. A global example of a current operational deployment of CV technology will be highlighted by examining the ITS SPOT program in Japan. Three basic services are offered there that have resulted in expedited traffic

---

[94] Jim Barbaresso et al., *Intelligent Transportation Systems ITS 2015–2019 Strategic Plan* (Washington, DC: U.S. Department of Transportation, 2014), http://www.its.dot.gov/strategicplan.pdf.

[95] Ibid.

[96] "Connected Vehicle Pilot Deployment Program; Request for Information," March 12, 2014, https://www.federalregister.gov/articles/2014/03/12/2014-05414/connected-vehicle-pilot-deployment-program-request-for-information.

flow, and have been identified as the causal factor contributing to a 60 percent reduction in accidents at a specific high crash area.[97]

Lastly, future developments in CV technology will be offered with discussion regarding preliminary policy guidance and the formation of coalitions to further research. Obstacles to deployment will also be briefly mentioned with corresponding strategies for solutions.

A.   CONNECTED VEHICLE TECHNOLOGY CONCEPTS AND BENEFITS

For well over a decade, the USDOT has engaged in research and testing of a connected vehicle platform.[98] The goal of this emerging technology is to allow vehicles to gather information relative to the vehicle's constantly changing environment both internal and external, and share that information wirelessly to other vehicles, infrastructure, and personal communicative devices like cell phones and tablets to improve safety, mobility, and environmental quality.[99]

Expectations from consumers have grown and the role of the motor vehicle in society has evolved from a simple physical system for safe, reliable transportation, to a mobile information platform capable of facilitating information flows in real time to support the modern connected lifestyle. A connected vehicle will take proactive measures to enhance safety and support driver awareness through applications like collision detection, lane changing, and cooperative management of traffic flow on the highways of the nation.[100]

There are a number of tangible benefits to be derived from this technology. Through research and development, new technologies and innovations promise more

---

[97] "ITS (Intelligent Transport System) Spot Services|International Transport Forum 2012 Summit," accessed May 18, 2015, http://www.mlit.go.jp/kokusai/itf/kokusai_itf_000006.html.

[98] "(USDOT) Releases a New Fact Sheet on Planning for the Future of Connected Vehicles and Intelligent Transportation Systems (ITS)," June 11, 2015, http://campaign.r20.constantcontact.com/render?ca=0ce83352-2b4b-48af-a6b1-ff7c0970d778&c=77da6f90-5104-11e3-8e6b-d4ae52a4597c&ch=7a7c1c80-5104-11e3-8e6c-d4ae52a4597c.

[99] Ibid.

[100] Ning Lu et al., "Connected Vehicles: Solutions and Challenges," *IEEE Internet of Things Journal* 1, no. 4 (August 2014): 289, doi:10.1109/JIOT.2014.2327587.

efficient and sustainable travel. Safety adherents tout a vast reduction in the number and frequency of motor vehicle crashes.[101]

According to the Transportation Research Board of the National Academies, "almost all transportation fatalities—approximately 94 percent occur on highways and mostly involve passenger vehicle crashes."[102] Fatalities and personal injury accidents are expected to decrease significantly as systems are fully integrated into society.

Another safety benefit expected is the proposed reduction in traffic congestion in metropolitan areas and the nation's highways. Mobility is expected to improve as real time traffic data can be disseminated to all drivers, commercial operators, and transportation officials to help alleviate congestion.[103] The 2012 Urban Mobility Report by Schrank and Lomax indicates the impact of traffic congestion on the individual. The study highlighted the cost to consumers and estimated the cost of congestion at 120 billion dollars or approximately $820 dollars per commuter in the United States.[104]

The reduction of congestion on the highway will be achieved through the platooning of vehicles.[105] This concept involves the reduction of spacing between all vehicles on the highway as they communicate with each other. Since each vehicle perceives what the other vehicles in the platoon are doing this increases traffic flow, and helps to eliminate the stop and go gaping which results from driver input in current traffic situations.

The gains achieved through greater mobility are also anticipated to have positive effects on the environment. Combustion engines produce emissions that include

---

[101] AASHTO Executive Committee, *AASHTO Connected Vehicle Field Infrastructure Footprint Analysis: Preparing to Implement a Connected Vehicle Future: Preparing to Implement a Connected Vehicle Future*, 2.

[102] Transportation Research Board of the National Academies, *Critical Issues in Transportation 2013*; "New VTTI Study Results Continue to Highlight the Dangers of Distracted Driving," accessed July 29, 2014, https://www.vtti.vt.edu/featured/052913-cellphone.html.

[103] AASHTO Executive Committee, *AASHTO Connected Vehicle Field Infrastructure Footprint Analysis: Preparing to Implement a Connected Vehicle Future: Preparing to Implement a Connected Vehicle Future*, 2.

[104] "Annual Urban Mobility Report," accessed July 29, 2014, http://mobility.tamu.edu/ums/.

[105] "The SARTRE Project," accessed September 1, 2015, http://www.sartre-project.eu/en/Sidor/default.aspx.

pollutants that are harmful to the atmosphere. Quality of life is affected by increases in pollutant levels caused by traffic congestion. Connected vehicle technology is expected to produce reductions in fuel consumption, idling motors, and vehicle miles travelled all of which can have an adverse impact on the environment.[106]

B.   STAKEHOLDERS, THEIR ROLES, TERMINOLOGY

The concept of connected vehicle technology, when fully implemented, will transition the motoring public from being isolated individual entities into a collective body creating an inter-connected vehicle community. These communities made up of vehicles, infrastructure, and personal electronic devices will communicate in real time providing critical information to all users. Information generated by the on-board vehicle computer, on-board sensors, or passenger devices can be effectively shared with vehicles in proximity, or to other vehicles in a network, so that traffic flow and other safety related data might be shared in a secured environment.[107]

Synchronized traffic flow and driver awareness are the ultimate goals and will lead to reduced accidents at intersections, increased mobility on the highway, increased efficiency in emergency response and expedited highway maintenance dispatch to problem areas as connected vehicles relay information to each other and organizations responsible for highway safety.[108]

The connected vehicle system is projected to include several elements as indicated by both the U.S. Department of Transportation (USDOT) and other involved organizations like the American Association of State Highway and Transportation Officials (AASHTO), and academics at major transportation affiliated universities.

According to the AASHTO Executive Committee, these elements include:

---

[106] "ITS Strategic Plan 2015–2019," accessed June 12, 2015, http://www.its.dot.gov/strategicplan/index.html.

[107] Ching-Yao Chan, "Connected Vehicles in a Connected World," in *VLSI Design, Automation and Test (VLSI-DAT), 2011 International Symposium on* (IEEE, 2011), 1–4, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5783569.

[108] Ibid.

- Roadside communications equipment like Dedicated Short Range Communication (DSRC) together with enclosures, mountings, power, and network backhaul running applications and systems responsible for a variety of services to include security.

- Traffic signal controller interfaces for applications that require signal phase and timing data.

- Systems and processes required supporting management of security credentials and ensuring a trusted network.

- Mapping services that provide highly detailed roadway geometrics, signage, and asset locations for the various Connected Vehicle applications.

- Positioning services for resolving vehicle locations to high accuracy and precision.

- Data servers for collecting and processing data provided by vehicles and for distributing information, advisories, and alerts to users.

- Technical standards in place to specify interfaces and messages between vehicles and infrastructure with network information services.

- A Security Certificate Management System with standardized interfaces is available to support trusted connected vehicle infrastructure deployments.[109]

They are in part driven by USDOT's requirements for infrastructure maintenance and improvements at state and local levels. A third party may implement security system design elements that could be provided by automakers if required by the National Highway Transportation Safety Administration (NHTSA).[110]

One of the biggest hurdles to overcome with connectivity is how to achieve a reliable wireless link when drivers and systems are relying on data for safety critical functions. In metropolitan areas for instance, vehicle to vehicle (V2V) communications

---

[109] AASHTO Executive Committee, *AASHTO Connected Vehicle Field Infrastructure Footprint Analysis: Preparing to Implement a Connected Vehicle Future: Preparing to Implement a Connected Vehicle Future*, 2.

[110] Ibid., 5.

can be difficult due to building obstructions and large volumes of vehicles sending and receiving data that could lead to signal disruptions or loss.[111]

As vehicles become connected, they will create vehicle ad hoc networks (VANET) which can be challenging due to the high mobility of vehicles in different trajectories and traversing various networks in quick succession.[112] The limited range of V2V communications can also lead to disruptions as vehicles encounter network partitions and obstacles, such as structures and large commercial type vehicles.[113] These negatives are offset to a degree by the fact that vehicles travel defined, well-mapped roadways where travel estimations can be reasonably calculated, and vehicles also possess strong computer processing capability with Global Positioning System (GPS) functionality and generate their own power.[114] Achieving the network capability can take many forms and several systems are currently under study. No determination has yet been reached by the U.S. Department of Transportation as to what communication system will be used for the connected vehicle program. Some options being considered for implementation follow.

C.   CURRENT STATE OF TECHNOLOGY

This section will examine the current state of connected vehicle technology by examining several system components and their functionality. It will also offer a brief discussion on systems security that is vital to user acceptance and will provide the springboard for operational deployment of this technology. It will explain how without secure systems the public will not accept that machines can provide any safer travel environment than can be accomplished today.

---

[111] Lu et al., "Connected Vehicles," 292.

[112] Ibid.

[113] Ibid.

[114] Ibid.

D. OPERATIONS

A connected vehicle will perform a number of independent functions seamlessly and combine this functionality through multiple sensors and onboard processing units linked to the various automotive control systems that will provide drivers safety awareness.[115] In essence, cars must be able to understand their environment, real-time, with sensors and know where it is, while communicating with other vehicles, infrastructure, and personal devices.[116]

Sensory information is communicated in order to reduce crashes, enable safety, and "provide continuous real time connectivity to system users."[117] Connected vehicles will scan in 360 degrees to inform the operator of hazards and situations they might not recognize.[118] These alerts should allow operators sufficient time to take corrective action in time to avoid collisions.

A recent NHTSA analysis projects that connected vehicle technology could lead to significant reductions in motor vehicle crashes upwards of 80 percent.[119] Enhanced mobility can be realized through more efficient decision making by vehicle operators and highway maintenance officials. As dynamic traffic scenarios are reported by connectivity, managers can re-route traffic quickly or dispatch resources to handle emerging issues more efficiently.[120]

---

[115] Lu et al., "Connected Vehicles," 289.

[116] AASHTO Executive Committee, *National Connected Vehicle Field Infrastructure Footprint Analysis* (Washington, DC: American Association of State Highway and Transportation Officials, 2013), 17, http://r.search.yahoo.com/_ylt=A0LEVv3jhqFUCAwAUwEPxQt.;_ylu=X3oDMTBybnV2cXQw BHNlYwNzcgRwb3MDMgRjb2xvA2JmMQR2dGlkAw--/RV=2/RE=1419900772/RO=10/RU=http% 3a%2f%2fssom.transportation.org%2fDocuments%2fApplications_Analysis%2520v3%2520july%252020 13.pdf/RK=0/RS=LfSpgJ63mKEdycufT2Vrxeg6eP8-.

[117] "Connected Vehicle Frequently Asked Questions," accessed July 18, 2014, http://www.its.dot.gov/ connected_vehicle/connected_vehicles_FAQs.htm.

[118] "U.S. Department of Transportation Announces Decision to Move Forward with Vehicle-to-Vehicle Communication Technology for Light Vehicles," accessed July 28, 2014, http://www.nhtsa.gov/ About+NHTSA/Press+Releases/2014/USDOT+to+Move+Forward+with+Vehicle-to-Vehicle+Communi cation+Technology+for+Light+Vehicles. National Highway Traffic Safety Administration (NHTSA).

[119] NHTSA, *Planning for the Future of Transportation: Connected Vehicles and ITS.*

[120] "Connected Vehicle Frequently Asked Questions."

With efficiency also comes a reduction on the environmental impact caused by traffic congestion. Options for re-routing a trip based on accumulated data from multiple vehicle systems sensing congestion or road blockage should increase fuel economy and minimize lost production time.[121]

Connected vehicle technology while not required for autonomous driving is expected to complement and enhance autonomy and provide increased societal benefit through reductions in traffic crashes, and enhanced driver awareness to facilitate a safer transportation system.[122] The basic core of connected vehicle technology rests in wireless connectivity between vehicles (V2V), infrastructure (V2I), and other mobile devices (V2X).[123]

Increasing use of wireless data communications has fundamentally changed society with its constant demand for instant access to information and infotainment systems. This access is now provided to users while in transit as consumers take advantage of infotainment systems integrated into new vehicles. The Connected Car Industry Report 2013 prepared by Telefonica cites a Machina Research report that indicates connectivity will be the norm in the year 2020, as 90 percent of new cars will be equipped with the technology as opposed to 10 percent today.[124]

Various wireless systems are currently under study to support the connected vehicle environment while benefiting society.[125] These benefits are highlighted by a projected reduction in highway traffic crashes that may translate into reduced fatalities and personal injuries. When real-time traffic information is known, mobility and efficiencies can be realized by all ground transportation sectors whether private or commercial.

---

[121] AASHTO Executive Committee, *National Connected Vehicle Field Infrastructure Footprint Analysis*, 2.

[122] Barbaresso et al., *Intelligent Transportation Systems ITS 2015–2019 Strategic Plan*, 14.

[123] AASHTO Executive Committee, *AASHTO Connected Vehicle Field Infrastructure Footprint Analysis: Preparing to Implement a Connected Vehicle Future*.

[124] Carlos Paulin et al., *Telefonica Digital Connected Car Report 2013* (London: Telefonica, 2013).

[125] AASHTO Executive Committee, *AASHTO Connected Vehicle Field Infrastructure Footprint Analysis: Preparing to Implement a Connected Vehicle Future*.

E. COMMUNICATION SYSTEMS—CELLULAR/WI-FI/DSRC

Communications systems all have unique attributes, which are being evaluated by researchers in an effort to identify the system that offers the greatest utility. These systems must be capable of providing functionality to a host of convenience features like Bluetooth, wireless, navigation, and infotainment systems that consumers currently demand.

Additional services include emergency roadside assistance, security services like remote access lock and start, and vehicle locator and tracking. These services will likely increase with technology improvements, and will be in addition to the basic safety communications that will occur in the connected environment.[126] A brief synopsis of each proposed system will be discussed.

There has been tremendous expansion in the cellular market with 3G (third generation) and newer 4G LTE(fourth generation Long Term Evolution) mobile devices becoming ubiquitous in society. These devices provide a standard for wireless communication and allow high-speed data to be uploaded to the mobile device.[127] This expansive presence coupled with robust cellular operating systems that include GPS capability represent a technology that can be used in fostering connectivity.[128]

There are multiple connectivity options to include Bluetooth, WI-FI, and 3G and 4G LTE services offering ultra-high speed, high bandwidth connectivity.[129] Mobile devices can be easily upgraded and customized to meet user specifications. People are familiar with and comfortable using their devices for numerous functions so using them in a vehicle setting will offer little challenge. New products emerging in the market allow hands free use of cellular devices. Two recent cell phone applications include the

---

[126] Chan, "Connected Vehicles in a Connected World."

[127] Sascha Segan, "3G vs. 4G: What's the Difference?," *PCMAG*, February 10, 2015, http://www. pcmag.com/article2/0,2817,2399984,00.asp.

[128] Lu et al., "Connected Vehicles," 294.

[129] Pedro Daniel Urbina Coronado et al., "Development of an Android OS Based Controller of a Double Motor Propulsion System for Connected Electric Vehicles and Communication Delays Analysis," Mathematical Problems in Engineering, accessed December 2, 2014, http://www.hindawi.com/journals/ mpe/2014/467165/abs/.

Android Auto app and Apple's CarPlay app. Each will allow safe use of cellular devices through the vehicle's interior display console while in motion.[130] Smartphone's are not limited to infotainment services as a recent journal article in the *International Journal of Vehicle Systems Modeling and Testing* outlined the use of a Blackberry phone to access information from the on-board diagnostic interface to provide driver awareness to emerging safety critical events or situations.[131]

In spite of all the possibilities for use of cellular technology, some major obstacles still exist. The requirement for standardized communication and performance standards being provided by multiple cellular companies may be problematic. Cellular companies must continue to upgrade coverage areas and infrastructure to achieve greater performance. Issues with delays in communications or signal loss will adversely affect system performance. Processing of data for vehicle decision-making and control will require real time capability; currently mobile devices are better suited for telecommunications, but not safety critical real-time tasks.[132]

Other wireless systems identified for consideration include Bluetooth technology. This short-range wireless service operates at 2.4 GHz.[133] It is currently utilized in a number of capacities, including hands free telephone service, and in wireless entertainment applications. It is a common feature in vehicles' mobile devices and other consumer electronics. Bluetooth eliminates the need for cables as data is transmitted wirelessly however; range of the technology is limited and high power settings are required to boost transmission.[134]

---

[130] Lu et al., "Connected Vehicles," 294.

[131] Johan Wideberg, Pablo Luque, and Daniel Mantaras, "A Smartphone Application to Extract Safety and Environmental Related Information from the OBD-II Interface of a Car," *International Journal of Vehicle Systems Modelling and Testing* 7, no. 1 (2012), http://trid.trb.org/view.aspx?id=1138025.

[132] Coronado et al., "Development of an Android OS Based Controller of a Double Motor Propulsion System for Connected Electric Vehicles and Communication Delays Analysis."

[133] Lu et al., "Connected Vehicles," 291.

[134] Ibid.

ZigBee technology is also a similar technology operating on 2.4 GHz.[135] The system contains multiple nodes that can preserve communications links in the event of a failure in any one node. The system searches for and reconnects to an active node thus ensuring the link while extending the range of the overall system.[136] It uses low power settings and offers security mechanisms like encryption while maintaining interoperability with other systems.[137] Difficulties in combating engine noise and interference from Bluetooth devices has been identified in studies.[138]

Radio frequency identification (RFID) technology has also been studied for possible use with sensor systems. Passive RFID tags mounted on sensors would be queried by signal from the tag reader mounted in the electronic control unit and the data received.[139] By using a passive RFID system, manufacturers could take advantage of low equipment costs, and are relieved of providing power supply to the RFID tags.[140] This system does have some negative attributes that include backup power to maintain continuous data flow when powered RFID systems suffer power loss.[141] This deficiency does not offer sound solutions for safety critical environments.

Two additional alternatives are identified as providing some options for connectivity. The first is ultra-wideband (UWB), or digital pulse, which is a wireless technology similar to Bluetooth that operates in the 3.1–10.6 GHz frequency that supports short range communications at an acceptable data rate and low energy level.[142] Large amounts of digital data can be transmitted over the broad spectrum at very low power at a very high rate. UWB broadcasts precise digital pulses, which require the

---

[135] Lu et al., "Connected Vehicles," 291.

[136] "ZigBee," accessed December 30, 2014, http://zigbee.org/.

[137] Ibid.

[138] Lu et al., "Connected Vehicles," 291.

[139] Ibid.

[140] Ibid.

[141] Ibid.

[142] A. S. Syed Navaz and G. M. Kadhar Nawaz, "Ultra Wideband on High Speed Wireless Personal Area Networkss," *International Journal of Science and Research (IJSR)*, accessed January 1, 2015, http://www.ijsr.net/archive/v3i8/U0VQMTQx.pdf.

synchronization of the equipment used to send and receive signals.[143] This precision leads to extremely high accuracy measured in trillionths of a second.[144]

The other identified wireless system is the 60 GHz Millimeter Wave also known as millimeter wave communications. It operates in the 57 - 64 GHz range and supports multi gigabytes per second wireless connections in a short range for multimedia applications.[145] Additionally, antennas at this level are small and directional and can be expensive.[146] Both the UWB and the 60 GHz millimeter wave applications show promise, but the major challenge for wireless systems is overcoming the communications environment both inside and outside the vehicle.[147]

The final system for consideration is referred to as dedicated short range communication (DSRC) by the Department of Transportation.[148] This system utilizes the 5.9 GHz spectrum, which was protected by the Federal Communications Commission for intelligent highways.[149] Identified uses of the system include:

- Traffic light control

- Traffic monitoring

- Traveler's alerts

- Automatic toll collection

- Traffic congestion detection

- Emergency vehicle signal preemption of traffic lights

---

[143] "Ultra-Wideband Technology," accessed January 1, 2015, http://www.bluetronix.net/Ultra_Wideband_Technology.htm.

[144] Ibid.

[145] Lu et al., "Connected Vehicles."

[146] Nan Guo et al., "60-GHz Millimeter-Wave Radio: Principle, Technology, and New Results," *EURASIP Journal on Wireless Communications and Networking* 2007 (2007): 1–8, doi:10.1155/2007/68253.

[147] Lu et al., "Connected Vehicles."

[148] "DSRC: The Future of Safer Driving Fact Sheet."

[149] "FCC Allocates Spectrum 5.9 GHz Range for Intelligent Transportation Systems Uses," accessed December 31, 2014, http://transition.fcc.gov/Bureaus/Engineering_Technology/News_Releases/1999/nret9006.html.

- Electronic inspection of moving trucks.[150]

DSRC allows for two-way wireless communications that will allow for safety critical data transfer between vehicles and infrastructure.[151] DSRC also provides immediate communication capability with capacity for frequent updates.

In order for data transfers to be effective low latency is required that allows data to be transmitted and received in milliseconds.[152] DSRC also allows for reliable service in high mobility situations and performs in varying weather conditions. The system also possesses security and privacy through safety message authentication.[153] Since the 1999 press release the benefits attributed to DSRC communications has expanded to include:

- Blind spot warning

- Forward Collision warning

- Sudden Braking ahead warning

- Do not pass warning

- Intersection collision avoidance

- Approaching emergency vehicle warning

- Vehicle safety inspection

- Transit or emergency vehicle signal priority

- Electronic parking and toll payment

- Commercial vehicle clearance and safety inspections

- Rollover warning

- Traffic and travel condition data[154]

Although multiple systems have been analyzed, the National Highway Transportation Safety Administration has given significant endorsement to DSRC as the

---

[150] "FCC Allocates Spectrum 5.9 GHz Range for Intelligent Transportation Systems Uses."

[151] "DSRC: The Future of Safer Driving Fact Sheet."

[152] Ibid.

[153] Ibid.

[154] Ibid.

premiere system for vehicle connectivity. This is evidenced by the decision in 2013 to seek a rulemaking for deployment of 5.9 GHz on-board equipment in light vehicles, followed by the 2014 decision to pursue a rulemaking for the technology in commercial vehicles.[155]

If NHTSA issues the rulemaking on safety applications then consumers may see vehicles equipped with DSRC in production by 2019. These vehicles would broadcast a basic safety message to include location, speed, and direction of travel.[156] According to U.S. Department of Transportation research of available communications networks, DSRC provides the best mechanism for transmission of safety critical information.[157] There is concern among advocates of the connected vehicle system that the FCC's consideration of sharing the dedicated spectrum with unlicensed equipment like cordless phones will cause problems with signal interference.[158] With the continued growth of WI-FI it is expected that with more devices broadcasting and receiving information, interference with safety communications could occur.

F.   SYSTEM SECURITY

Creating a secure environment for connected and autonomous vehicle technology is one of the highest priorities and is one of the objectives listed in policy guidance issued by NHTSA.[159] Electronic control systems safety will include measures and studies focused on "developing functional safety requirements, as well as potential reliability requirements in the areas of diagnostics, prognostics, and failure response (fail safe)

---

[155] AASHTO Executive Committee, *National Connected Vehicle Field Infrastructure Footprint Analysis*.

[156] Ibid., 2.

[157] United States Department of Transportation, *U.S. Department of Transportation Vehicle Research Program: Vehicle to Vehicle Safety Application Research Plan* (Washington, DC: United States Department of Transportation, 2011).

[158] John Harding et al., *Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application* (Washington, DC: NHTSA, 2014).

[159] "NHTSA V2V Communications," accessed July 28, 2014, http://www.safercar.gov/v2v/v2v.html.

mechanisms. In addition, NHTSA has initiated research on vehicle cybersecurity, with the goal of developing an initial baseline set of requirements."[160]

A Public Key Infrastructure (PKI) system has been identified as a viable means of securing the communications between vehicles, the infrastructure, and mobile devices. Public key cryptography was created in 1976 by Whitfield Diffe, cryptographer and Stanford graduate student and Martin Hellman, Professor Emeritus at Stanford University. Their paper *New Directions in Cryptography* emphasizes an asymmetric process for encryption and decryption.[161] The public key infrastructure process consists of the computerized components and policies necessary to create, manage, store, issue and revoke digital certificates.[162] This system includes a certificate authority (CA), which issues the digital certificate after receiving verification from the registering authority (RA); in addition, a directory maintains the digital certificates. A PKI system can be used in various applications, such as email and computer programs that require encryption.

The certificate distribution and management system concept calls for the use of two keys, one is private and remains secret while the other key is public and can be shared. The two keys can only be used with each other because of algorithms, to encrypt and decrypt information.[163] This mathematical relationship creates a key pair, and ensures integrity and prevents one key from being used to identify the other or from undoing an operation. As a result, information encrypted using a public key can be decrypted using the private key that is paired with the public key. This asymmetric process allows one entity to use the same key pair with various entities instead of creating different keys for each transmission.[164]

---

[160] "U.S. Department of Transportation Releases Policy on Automated Vehicle Development."

[161] "Understanding Public Key Cryptography," accessed November 16, 2014, 1, http://technet.micro soft.com/en-us/library/aa998077(v=exchg.65).aspx.

[162] Anita Kim et al., "An Approach to Communications Security for a Communications Data Delivery System for V2V/V2I Safety: Technical Description and Identification of Policy and Institutional Issues," 14, November 2011, http://trid.trb.org/view.aspx?id=1131372.

[163] "Understanding Public Key Cryptography," 1.

[164] Ibid.

In the case of connected vehicle systems, the digital certificates issued by the CA will be encrypted and decrypted using a PKI system. Digital certificates guarantee validity of the information contained in the message.[165] As a safety measure, digital certificates are only valid for a brief, specific time and contain the public key of the entity identified in the certificate, without revealing the user's personally identifying information.[166] Security is enhanced as certificates support anonymity by issuing random pseudonyms as temporary identifiers and is proposed to be valid for a single, pre-determined five-minute period.[167] By issuing certificates with thirty-second overlaps from the beginning and ending times, a vehicle is ensured access to a valid certificate. These two-way trusted and secure communications also provide for certificate revocation lists that can be used to revoke certificates of misbehaving actors.[168] Additional safety enhancements in connected vehicles can be made to hardware systems on the vehicle through tamper proof design and in software code, which can identify misbehavior in systems performance.[169] Testing these concepts is ongoing in a series of test beds operated by the transportation institutes of major universities located in the United States.

G.   CONNECTED VEHICLE DEPLOYMENT TESTING

The U.S. Department of Transportation is currently sponsoring a Connected Vehicle Safety Pilot Model Deployment research program that is multimodal and aims to enable a safe, connected environment between vehicles, infrastructure, and personal mobile devices using wireless communications systems.[170] Connected vehicle test beds provide the vehicle to vehicle and vehicle to infrastructure communications system for

---

[165] "Understanding Digital Certificates," accessed November 16, 2014, http://technet.microsoft.com/en-us/library/bb123848%28v=exchg.65%29.aspx.

[166] Ibid., 1; Kim et al., "An Approach to Communications Security for a Communications Data Delivery System for V2V/V2I Safety," 31.

[167] Kim et al., "An Approach to Communications Security for a Communications Data Delivery System for V2V/V2I Safety," 32.

[168] Ibid., 16.

[169] Ibid.

[170] "Safety Pilot Model Deployment: Connected Vehicles," 2012, YouTube video, 3:11, posted by Quentin Weir, July 16, 2012, https://www.youtube.com/watch?v=hVyS6btjxhI&feature=youtube_gdata_player.

testing. Testing is designed to determine how effective safety applications are at reducing crashes, and driver responses to those applications.[171] Some features of the testing include driver awareness functions that track vehicle position and issue alerts to drivers on congestion, road blockage, weather related information, and emergency vehicle presence. This information can be relayed to similarly equipped vehicles and mobile devices when fully functional.

An organization of affiliated test beds has evolved through the ITS Joint program office.[172] Memorandums of agreement have been signed by sixty-one public, private, and academic organizations to exchange accumulated data.[173] These test bed experiments will aid in the development of common platforms and expand learning on connected vehicle components. There are currently five operational test beds that are located in Virginia, California, Florida, and two sites in Michigan.[174] An examination of two test beds, in Michigan and Virginia will be offered in brief.

1.   Virginia Connected Corridors

The Commonwealth of Virginia is participating in real world research and testing of connected vehicle technologies along portions of the interstate system on I-66 and I-495 and along primary routes, U.S. 29 and U.S. 50 in the extremely congested area of Northern Virginia.[175] Included in the corridor system is the Virginia Smart Road Center located in Blacksburg, Virginia, which was created in 2002 from a partnership between Virginia Tech and the Virginia Department of Transportation.[176] This full-scale research

---

[171] Walton Fehr et al., "Southeast Michigan 2014 Test Bed Project for Connected Vehicles: The Next Step toward Deploying ITS," in *Connected Vehicles and Expo (ICCVE), 2013 International Conference on* (IEEE, 2013), 66–70, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6799771.

[172] "Intelligent Transportation Systems—Test Beds," accessed January 6, 2015, http://www.its.dot.gov/testbed/testbed_affiliated.htm.

[173] Ibid.

[174] Ibid.

[175] "Virginia Connected Corridors," accessed August 10, 2015, http://www.apps.vtti.vt.edu/PDFs/VCC.pdf.

[176] "The Smart Road," accessed August 10, 2015, http://www.roadstothefuture.com/Smart_Road.html.

facility offers a two lane highway multi-purpose test bed 2.2 miles long for testing of new transportation technologies.

The corridor system contains sixty embedded roadside equipment units that are capable of transmitting driver awareness information in the form of infrastructure reports or to receive DSRC messages routed from vehicles in close proximity.[177] These applications are instrumental in providing real time traveler information on lane closures, traffic congestion, work zone and incident management data that would allow connected motorists to make informed decisions for traffic route planning with the byproduct being safety and improved mobility in a congested environment. Transportation officials could likewise make decisions regarding roadway repairs and transit operations that improve safety for all motorists.

2.   Mobility Transformation Center—Michigan

The U.S. Department of Transportation partnered with the University of Michigan in 2012 to conduct a 31 million dollar project to evaluate connected vehicle technology.[178] The project involved around 3,000 vehicles in the Ann Arbor area as the streets became a connected vehicle test bed.[179] Cars, trucks, and buses were equipped with the technology, as well as infrastructure at selected sites in the area. The test bed proved to be a success and the data transmitted was captured to provide an overall assessment, on a large scale, as to the viability of this technology.[180] Currently plans are to increase the number and location of additional test bed projects across the nation. Recently the University announced plans to expand the number of vehicles involved in

---

[177] AASHTO Executive Committee, *AASHTO Connected Vehicle Field Infrastructure Footprint Analysis: Preparing to Implement a Connected Vehicle Future*, 5.

[178] "University of Michigan Mobility Transformation Center," accessed August 10, 2015, http://www.mtc.umich.edu/partners/government.

[179] Ibid.

[180] Ibid.

testing to 9,000 with an expected 100 million dollars spent on vehicle to vehicle research by the year 2022.[181]

While both of these projects currently are considered test beds it is anticipated that testing will eventually lead to these roadways becoming operational in the future as the technology is proven and gains user acceptance.[182] It is also worthwhile to learn what other countries are doing with respect to this technology in order to create best practices for implementation. The country of Japan has an operational connected vehicle system deployed and in use today.

H.   JAPAN INTELLIGENT TRANSPORTATION SYSTEM (ITS) AND ITS SPOT SERVICE

The country of Japan spans over 145,000 square miles and has a population in excess of 127 million. Approximately 67 percent of the residents live in cities creating traffic congestion and emissions issues, which affect health and well-being.[183]

With respect to the promotion of intelligent transportation systems to the full Japanese cabinet there are four ministries that receive information from the Japanese ITS Standardization Committee and ITS Japan which is comprised of industry and academia.[184] These ministries promote the objectives of the Japanese ITS Comprehensive plan.

- Ministry of Land, Infrastructure, Transport and Tourism

- National Police Agency

- Ministry of Internal Affairs and Communications

---

[181] "Connected Vehicles: U.S. DOT Launches Community Resource Website for Connected-Vehicle Pilot Programs," accessed January 6, 2015, http://www.roadsbridges.com/connected-vehicles-us-dot-launches-community-resource-website-connected-vehicle-pilot-programs.

[182] "Virginia Tech Transportation Institute and Partners Unveil Virginia Automated Corridors," accessed August 10, 2015, http://www.vtti.vt.edu/featured/?p=260.

[183] "Fast Facts: Japan," accessed May 19, 2015, http://www.scholastic.com/teachers/article/fast-facts-japan.

[184] "ITS (Intelligent Transport System) Spot Services|International Transport Forum 2012 Summit."

- Ministry of Economy, Trade, and Industry[185]

Traffic safety is a major theme in Japan as the country reports approximately 5,000 traffic fatalities per year.[186] Economic losses due to traffic congestion in the highly urbanized areas are calculated annually at 12 trillion yen (136 Billion).[187] Japan has a long history of technological innovation across a broad array of systems to include aircraft, computer technology, and motor vehicles.

The concept of an Intelligent Transportation System (ITS) has been studied in Japan since the early 1970s.[188] The evolution of multiple studies spanning a two-decade period led to the development of the *Vehicle Information and Communication System (VICS)*.[189] The system presents drivers with traffic and travel information to enhance situational awareness of emerging road conditions throughout the country.

Examples of safety data transmitted include traffic congestion, road construction, and traffic accident information.[190] Drivers alerted to hazardous conditions can make reasoned judgments regarding travel/commuting plans that can increase productivity, alleviate traffic delays, and decrease detrimental environmental concerns of increased gasoline consumption and increased emissions.[191] By showcasing available service and parking areas to consumers, the VICS system is able to expedite service delivery in private and commercial operations.[192]

Another ITS structure formed in Japan is the *Vehicle, Road and Traffic Intelligence Society (VERTIS)*.[193] Formed in the early 1990s the group is comprised of a

---

[185] "ITS (Intelligent Transport System) Spot Services|International Transport Forum 2012 Summit."

[186] Ibid.

[187] Ibid.

[188] Michigan Department of Transportation and Center for Automotive Research, *International Survey of Best Practices in Connected and Automated Vehicle Technologies 2013 Update* (Ann Arbor, MI: Michigan Department of Transportation & The Center for Automotive Research, 2013).

[189] Ibid.

[190] Ibid., 31.

[191] Ibid.

[192] Ibid.

[193] Ibid.

consortium of government entities, academia, and industry representatives, which led to the creation of a framework for intelligent transportation systems.[194] The significance of the consortium was evidenced in a name change in 2001 to "ITS Japan" and more importantly, the establishment of a cabinet level IT Strategic Headquarters within the Cabinet Secretariat. This high-level entity sanctioned by the government keeps Japan relevant in the telecommunications technology realm while promoting advanced information and telecommunications networks.[195]

In 2006, the IT Strategic Headquarters produced a design document of the overall IT plan, which stressed the need for mutual cooperation of public/private sectors in order to reduce crash severity, injuries, and fatalities while improving response times to such events. The system identified to achieve the goal outlined in the design document is the ITS Spot Service.

I.   ITS SPOT SERVICE

ITS Spot Service began in 2011 as a nationwide deployment of roadside devices that transmit and receive messages.[196] Over 1600 devices have been erected. The system connects with equipment installed on motor vehicles to provide safety awareness to drivers through the in-vehicle infotainment systems. It is anticipated that vehicle manufacturers will produce over 10 million on-board units that are ITS Spot compatible over a 5-year period.[197]

The system provides three basic services:

- Dynamic Route Guidance (DRG)

- Driving Safety Support Systems (DSSS)

- Electronic Toll Collection (ETC)[198]

---

[194] Michigan Department of Transportation and Center for Automotive Research, *International Survey of Best Practices in Connected and Automated Vehicle Technologies 2013 Update*, 31.

[195] Ibid.

[196] "ITS (Intelligent Transport System) Spot Services|International Transport Forum 2012 Summit."

[197] Ibid.

[198] Ibid.

Dynamic Route Guidance provides users with real time traffic information throughout the coverage area. Travel time data for all segments of highway will be transmitted from roadside units to on-board units. Once congestion points are identified, the car's navigation system uses the data to select alternate routes so that the road network is optimized and facilitates smoother traffic flow.[199] This technology was cited as producing a 60 percent decrease in accidents at one location on the expressway through Tokyo.[200] An unexpected benefit from the technology was realized as the ITS Spot Service was also instrumental in providing road closure information and real time warnings during a 2011 earthquake which hit Japan.[201] The data provided critical information to citizens and public safety response personnel on which routes to use expediting evacuation and response efforts.

The roadside equipment that facilitates the sharing of data in Japanese connected highway systems is referred to as Driving Safety Support Systems (DSSS).[202] The Universal Traffic Management Society within the National Police Agency of Japan monitors the DSSS project. The system supports safe driving by alerting operators of obstructions one-kilometer from the blockage. Congestion warnings are also produced that can give warning beyond visual range and even around curves. Images are produced that provide situational awareness of hazardous road conditions like snow, fog, and other weather related events. In order to provide maximum coverage of the road system ITS Spot units will be deployed systematically along the highway.

Tests of the connected vehicle system by car manufacturers have been undertaken with one such test involving 100 vehicles that utilized communications from infrastructure to determine if accident rates were lowered at dangerous intersections.[203] Cars were equipped with recorders and captured data from stop signs and traffic signals

---

[199] "ITS (Intelligent Transport System) Spot Services|International Transport Forum 2012 Summit."

[200] Michigan Department of Transportation and Center for Automotive Research, *International Survey of Best Practices in Connected and Automated Vehicle Technologies 2013 Update.*

[201] Ibid., 32.

[202] Ibid.

[203] Ibid.

to determine if connected technology would affect accident rates at designated high-risk intersections.[204] The program remained in place for six months and information would be transmitted to on-board vehicle display systems alerting drivers to roadway congestion and conditions. This situational awareness information resulted in driver's being alerted to congestion and hazardous conditions prior to arrival at the intersection.

Understanding how the vehicle and human operator will interface was also studied. The Nissan Corporation conducted tests of its vehicle to infrastructure communication system by using a naturalistic study involving approximately 2000 people.[205] This study was a validation trial of their ITS technology and results of the study are important to gauge responses by human operators when warning information is displayed.

Japan relies heavily on toll roads and the ETC system facilitates smooth traffic flow.[206] Upwards of 90 percent of transactions are processed by ETC.[207] In excess of 40 million toll transponders record roughly 5.6 million daily transactions.[208] This system helps to eliminate tollgate congestion and cuts carbon dioxide emissions by approximately 210,000 tons per year.[209] These tolls provide considerable funding for the connected technology systems throughout Japan.

A comparison can be drawn between the deployed system in Japan and the current system under study in the United States. The American test beds and the operational systems in Japan have demonstrated that connected technology does provide situational awareness to drivers. Alerts that provide notice of congestion and safety

---

[204] Michigan Department of Transportation and Center for Automotive Research, *International Survey of Best Practices in Connected and Automated Vehicle Technologies 2013 Update*, 33.

[205] Ibid.

[206] "Highlighting JAPAN," accessed May 18, 2015, http://www.gov-online.go.jp/eng/publicity/book/hlj/html/201208/201208_03.html.

[207] Michigan Department of Transportation and Center for Automotive Research, *International Survey of Best Practices in Connected and Automated Vehicle Technologies 2013 Update*.

[208] Ibid.

[209] "Highlighting JAPAN."

critical information have been recorded during testing.[210] Practical demonstrations of utility and safety enhancement for travelers in both nations are being put into practice. Additionally, an added benefit was realized when the technology was used by emergency management officials during preparedness and response to an actual natural disaster.[211]

J.   FUTURE DEVELOPMENTS IN THE UNITED STATES

The National Highway Transportation Safety Administration in August 2014 began the process of initiating a rulemaking to require the installation of the technology in all new light vehicles.[212] It will take many years for connected vehicles to become ubiquitous as most consumers maintain vehicles for a long period of time.[213] Aftermarket suppliers and installers will attempt to fill the gap by offering to modify a non-connected vehicle into a connected vehicle.[214]

Connected technology does have promise and is being rapidly advanced as Secretary Foxx of the U.S. Department of Transportation announced in May 2015 that NHTSA will move ahead of its proposed timetable for a proposed rule on vehicle to vehicle connectivity.[215] If the proposed rulemaking requiring that new vehicles be equipped with connected vehicle technology is issued as expected in 2016, then consumers may be able to purchase those vehicles by 2019.[216]

The Federal Highway Administration will also be providing guidance in the summer of 2015 to state transportation officials on adapting roadside equipment to be

---

[210] Michigan Department of Transportation and Center for Automotive Research, *International Survey of Best Practices in Connected and Automated Vehicle Technologies 2013 Update*, 33.

[211] Ibid., 32.

[212] "U.S. Department of Transportation Announces Decision to Move Forward with Vehicle-to-Vehicle Communication Technology for Light Vehicles."

[213] "GAO Study: Vehicle-to-Vehicle Technologies Expected to Offer Safety Benefits, but a Variety of Deployment Challenges Exist," November 2013, http://www.autosafety.org/gao-study-vehicle-vehicle-technologies- expected-tooffer-safety-benefits-variety-deployment-challenge.

[214] Ibid., 18.

[215] "(USDOT) Releases a New Fact Sheet on Planning for the Future of Connected Vehicles and Intelligent Transportation Systems (ITS)."

[216] Ibid.

compatible with connected vehicles. A draft of the document was completed in September 2014.[217]

The Vehicle to Infrastructure Deployment Coalition formed earlier in 2015 will consist of five Technical Working Groups focusing on V2I activities. The working groups will study:

- Deployment initiatives

- Deployment research

- Infrastructure operator

- OEM and supplier partnerships

- Deployment guidance

- Deployment standards[218]

The coalition held its first workshop meeting in Pittsburgh, Pennsylvania on June 4–5, 2015, and included the American Association of State Highway and Transportation Officials (AASHTO), the Institute of Transportation Engineers (ITE), and the Intelligent Transportation Society of America (ITS America).[219]

While the future is bright for connected vehicle technology many hurdles to deployment must be overcome. Safety proponents tout the potential for significant reduction in accidents but that position is couched in having all vehicles equipped with the technology and an operational system deployed with low latency required for safety critical information to be transmitted vehicle to vehicle and between vehicles and infrastructure.[220]

---

[217] "Public Meeting Seeking Stakeholder Input to Federal Highway Administration's Vehicle to Infrastructure (V2I) Deployment Guidance," accessed August 10, 2015, http://www.ops.fhwa.dot. gov/resources/news/v2istakeholdermtg.htm.

[218] "V2I Deployment Coalition Workshop: June 4–5, 2015," accessed May 20, 2015, http://www.itsa. org/index.php?option=com_forme&fid=103&Itemid=99999.

[219] Ibid.

[220] "GAO Study: Vehicle-to-Vehicle Technologies Expected to Offer Safety Benefits, but a Variety of Deployment Challenges Exist," 15–18.

The durability and the expected service life of the equipment are at this point also unknown.[221] As more research and technological development continues product sustainability should increase as more systems are used in test beds and real world conditions.

Protecting the system from cyber intrusion is another vital area requiring continued research.[222] There are many government, private, and academic institutions engaged in continued research of cyber related issues. The difficulty in securing this system is that requirements have not yet been fully identified and formalized. There are several options for delivering connected services and all will have to be defended.

The evolution of an intelligent transportation system in the United States will be gradual over the period of the next decade. Comprehensive studies are underway by government agencies, academic institutions, and private stakeholders to examine and further develop the technology prior to actual deployment. In the meantime, automobile manufacturers are introducing driver assistance systems in most new vehicles, which are the initial steps along the road to autonomy.

K.   CONCLUSION

The technology is poised to have significant societal benefit and when implemented should produce a significant reduction in highway traffic crashes, injuries, and fatalities. The systems should be studied fully to ensure unintended consequences are avoided that would be detrimental to deployment of this technology. A collaborative effort between policymakers, academics, legal professionals, and technical experts will provide the best framework of a multidiscipline approach to developing best practices.

The deployment of a fully functional ITS system in the United States will impact every facet of the ground transportation system. The available data on successful programs conducted on an international basis warrants inclusion and consideration as research and development continue in this field.

---

[221] Chan, "Connected Vehicles in a Connected World."

[222] Ibid.

With the given timeline for deployment of connected vehicle technology and the statements given by CEO's of major car manufacturers for offering self-driving cars within the next decade, there are questions that law enforcement agencies across the nation must address concerning regulation, legislation and operations that will require serious consideration and effective policy making in order to continue to fulfill mission requirements. These subject areas will be the focus of the following chapter.

THIS PAGE INTENTIONALLY LEFT BLANK

IV.   GOVERNMENTAL IMPACTS AND RESPONSE

The previous chapters offer the reader a macro level view of the technical aspects of the technology and what potential it may afford a consumer. This chapter will focus on outcomes along with organizational and governmental responses at the federal, state government level and will include changes necessary for effective law enforcement policy decisions. The emergence of autonomous and connected vehicle technology will require change in the regulatory, legislative, and operational processes for each of these sectors in the near future.

Having an understanding of the technology components and how they operate will move the discussion now, to how the world in which we operate as homeland security practitioners will be impacted in the three identified arenas of regulation, legislation and operations. This chapter will first discuss the impact at the federal level, and move to state level considerations with particular emphasis placed on the Commonwealth of Virginia. Lastly, the role of law enforcement will be analyzed as substantial change will be required for all governmental levels of public safety providers.

Some fundamental questions abound regarding regulation, legislation, and operations. For example, with respect to legislation is it even necessary? Car manufacturers will argue against it, yet responsible government requires it at least to some degree as public safety is directly involved. To what level then will regulation be required, and can it be implemented without stifling research and development?

Funding for research in autonomous and connected vehicle technology is provided by the federal government, yet current fiscal policy has resulted in stagnation for transportation issues.[223] Congress has failed to fully fund the Highway Trust Fund, which provides money to state and local governments for infrastructure maintenance and improvements. A well-maintained roadway with clearly identifiable lane markings and

---

[223] "Reports Highlight Weakened Federal, State Investment in Roads, Transit Systems," February 27, 2015, http://www.aashtojournal.org/Pages/022715spendinglevel.aspx.

signage is critical to the operation of autonomy in motor vehicles. Without consistent funding state maintenance will be cancelled or seriously delayed.[224]

Likewise, the landscape of legislation across the nation will require change as this technology evolves and gains user acceptance. Will a hodgepodge of legislation be crafted at the federal level, and across the fifty states that will serve to limit the utility of the technology by creating barriers to its deployment? Current legal definitions will also require amendment and existing statutes regarding "driver" responsibilities will undergo revision to reflect substantive change. As upper levels of autonomy are introduced the role of a "driver" evolves to that of a "user" and traffic/ criminal enforcement codes must also reflect the expansion of that role.

As regulation and legislation changes so too must operational elements like homeland security practitioners, who are charged with the protection of the United States and responsible for day to day enforcement of rules and regulations. Law enforcement agencies all across America will be affected and will need to evaluate their mission requirements and needs in light of this new technology that will alter the entire ground transportation system.

How will operational elements shift responsibilities and what new priorities will emerge and demand attention? It would be naïve to suggest that this emerging technology will always have a positive effect on society and never be used for illegal or immoral purposes.

Throughout the nation's history we have seen how new technologies like the automobile, computers, pharmaceuticals, and the Internet have emerged, provided societal benefit, and have then fallen victim to use by nefarious actors who learn to use the systems to expand criminal activities and subvert legal justice systems worldwide. This technology will no doubt follow the same path. Homeland security professionals must have vision to develop effective response protocols to fulfill their public safety mission requirements.

---

[224] "Wright Takes States' Case to Capitol Hill as Time Nears for Decisions on Trust Fund," April 17, 2015, http://www.aashtojournal.org/Pages/041715washpolicy.aspx.

The development of public policy to address the homeland security threat posed by rogue actors on this emerging technology is critical given the abbreviated timeframe projected by manufacturers for operational deployment of higher levels of autonomy in vehicles. There is limited guidance issued by the federal government regarding development and operational use of these vehicles. The state level guidance is restricted to licensing and operations. Currently, statutory authority to license or operate these vehicles is limited to Washington, DC, Nevada, California, Michigan, and Florida.[225] States like Virginia must take a proactive stance regarding policy development so that tangible benefits can be maximized and agencies like the Virginia State Police can fulfill their law enforcement responsibilities.

A.   THE GOOD AND THE BAD

There are a number of tangible benefits to be derived from this technology. Through research and development innovation will occur resulting in greater transportation efficiency. Law enforcement officials should also have access to data generated by these systems provided legal, privacy and regulatory mandates are met under close scrutiny by independent court officials.

Legally authorized and appropriate use by law enforcement of this information could aid in searches for individuals who are the subject of Amber or Silver alerts. The same methodology could be used to support criminal investigations of violent crimes like carjacking, or investigations with any connection to a motor vehicle.

Federal Bureau of Investigation Uniform Crime Report statistics indicates that a motor vehicle is stolen every 40 seconds in the nation.[226] Investigation of these crimes is difficult as indicated in the same report that in 2009 only 12.4 percent of cases were cleared by arrest or other means.[227] Using this new technology, once the vehicle identification number of the stolen vehicle is entered by a law enforcement agency, then the connected vehicle system would identify the last known location of the vehicle and an

---

[225] Anderson et al., *Autonomous Vehicle Technology: A Guide for Policymakers*, Product Page, xviii.

[226] "Statistics," accessed October 3, 2015, http://www.auto-theft.info/?page_id=49.

[227] Ibid.

investigation could immediately commence. Further research is required to ensure privacy rights and principles are not violated however. Administrative subpoenas or search warrants are currently required for other technologies (cellular phone, email) when similar requests for access and analysis are made.[228]

Technology is not always seen in a positive light, especially when computer systems fail causing delays in productivity or property loss. Autonomous vehicle technology will be evaluated in the same way. While it is anticipated that this emerging field will provide positive societal impacts there are counter arguments related to those benefits which must be examined, including the potential for the technology to enhance fraud, and vulnerability to cyber intrusion or criminal abuses.

This technology could also be used for nefarious purposes. One potential criminal use involves insurance fraud. FBI estimates exceed 40 billion per year for non-health related fraud.[229] For the foreseeable future, a mixture of autonomous and non-autonomous vehicles will occupy the nation's roadways. This environment may allow the staging of accidents between autonomous vehicles and those being operated by human drivers. Law enforcements ability to forensically examine autonomous systems at the scene of any incident is currently restricted as no equipment is currently designed for data downloading or determination of system status.

As connected vehicle and autonomous vehicle technologies are put into production, criminal elements are likely to attempt cyber attacks on the communications systems in order to file fraudulent insurance claims. The obvious concern with this technology is that it is reliant on a wireless environment. The protection of the data exchanged among vehicles, infrastructure and passengers' personal communication

---

[228] "§ 19.2-10.2. Administrative Subpoena Issued for Record from Provider of Electronic Communication Service or Remote Computing Service," 2, accessed November 30, 2015, http://law.lis. virginia.gov/vacode/19.2-10.2/; "§ 19.2-70.3. Obtaining Records Concerning Electronic Communication Service or Remote Computing Service," 2, accessed November 30, 2015, http://law.lis.virginia.gov/vacode/ 19.2-70.3/.

[229] "Insurance Fraud," accessed October 3, 2015, https://www.fbi.gov/stats-services/publications/ insurance-fraud/insurance_fraud.

devices from cyber intrusion must be safeguarded with fail safe systems designed to reduce the possibility of intrusion.[230]

There are several ways cyber security of autonomous vehicles can be illustrated as a national security concern. Kidnapping for profit has exploded globally and reports indicate in excess of 500 million dollars annually is garnered by criminal organizations.[231] These criminal elements could, with this technology, orchestrate political kidnappings of diplomats from foreign countries, or witnesses involved in criminal prosecutions. Current methods of hijacking require the perpetrators to engage the target directly at the scene. By using cyber intrusion to remotely hijack vehicles the perpetrators could reroute vehicles to predetermined locations where occupants would become vulnerable thereby removing themselves directly from the scene. The more control placed into the hands of the kidnappers as to time and place of the crime the greater the likelihood of success.

Another area where autonomous vehicles can be used to support criminal activity is by drug trafficking organizations smuggling drugs, weapons, or other contraband. Profits from illegal drug activity are significant. Seizures of drugs and assets by Drug Enforcement Administration (DEA) personnel over the eight-year period 2005–2013 have been valued in excess of 25 billion dollars.[232]

Currently drug organizations must occupy and accompany drug shipments to ensure arrival. With autonomy in vehicle operations, human involvement in the process of shipping narcotics or contraband can be significantly reduced. This process would benefit drug trafficking organizations by reducing exposure to law enforcement. For example, autonomous vehicles could inadvertently support this type of criminal activity as they are programmed to fully comply with existing traffic laws. Officers must rely on a

---

[230] Kim et al., "An Approach to Communications Security for a Communications Data Delivery System for V2V/V2I Safety: Technical Description and Identification of Policy and Institutional Issues."

[231] Rachel Briggs, *The Kidnapping Business* (London: The Foreign Policy Center, 2001), 1, fpc.org.uk/fsblob/46.pdf.

[232] "DEA Fact Sheet," accessed July 29, 2014, http://www.justice.gov/dea/docs/factsheet.pdf.

specific traffic/criminal violation or possess reasonable suspicion to justify to the courts a reason for making a traffic stop. An autonomous vehicle obeying all traffic laws could make it problematic for officers to justify to a court the reasonable basis for conducting a traffic stop.

B.   EXISTING TECHNOLOGY

We need look no further than existing technologies to see examples of how bad actors have created unintended consequences and influenced policy and strategy. Because autonomous vehicles by virtue of connectivity have a broad attack surface it is the threat of cyber attacks on the smart systems the vehicles employ that is a national security concern.[233]

Hackers are attracted to new technologies and are gratified and challenged by breaking into systems. While deviant, they often perform a valuable public service by exploiting weaknesses in systems that were previously unknown by vendors.[234] For example, low technology items like electronic toll collection systems with transponders have been hacked by monitoring the transactions of legitimate transponders and cloning similar devices for use in other vehicles.[235] Smart parking meter systems have similarly been hacked when the smart cards with stored value were monitored during transactions and custom smartcards were created to allow unlimited parking.[236]

Another example of a technology that has been used contrary to its original intended purpose is the mobile cell phone. While allowing unlimited communication opportunities worldwide these devices have also been used as triggers for improvised

---

[233] Anderson et al., *Autonomous Vehicle Technology: A Guide for Policymakers.*

[234] "Cybersecurity and Resiliency," accessed September 9, 2014, http://2013.vehicleautomation.org/ program/breakouts/cybersecurity.

[235] "FasTrak Talk Summary and Slides," accessed September 2, 2014, http://rdist.root.org/2008/08/ 07/fastrak-talk-summary-and-slides/.

[236] "Smart Parking Meters," accessed September 2, 2014, http://www.grandideastudio.com/portfolio/ smart-parking-meters/.

explosive devices.[237] The technology has also been seen to be viable as a weapon itself as Israel has even used a cell phone as an explosive device, triggered by making/ receiving a call, to assassinate the mastermind behind suicide attacks against Israelis.[238]

A concern of either technology is they also have the potential for release of personally identifying information. Although preliminary protocols make use of arbitrary or random identifiers, privacy concerns by consumers and watchdog groups must be addressed as technologies evolve. As systems undergo continuous development, patches or updates must be provided to ensure the highest levels of security are maintained.[239] The supplemental data used to update the systems or attacks carried out on data entry ports will be a logical place for hackers to infiltrate.[240]

C.   DEPLOYMENT CHALLENGES

There are several barriers to full implementation of autonomous vehicles, but not all concern national security. For example, cost to the consumer will be initially exorbitant. One estimate by the Eno Center for Transportation projected the cost of initial autonomous vehicles at $100,000 dollars.[241] Questions surrounding insurance liability issues for vehicle manufacturers have yet to be addressed. Manufacturers want strict limits placed on potential liability as this new technology is introduced. If limits remain high or unlimited there would be no incentive for continued research and development which would lead to safer and lower cost technology.[242]

---

[237] "NCJRS Abstract," accessed August 7, 2014, https://www.ncjrs.gov/App/Publications/abstract. aspx?ID=189403.

[238] Gal Luft, "The Logic of Israel's Targeted Killing," *Middle East Quarterly*, January 1, 2003, http://www.meforum.org/515/the-logic-of-israels-targeted-killing.

[239] Kim et al., "An Approach to Communications Security for a Communications Data Delivery System for V2V/V2I Safety: Technical Description and Identification of Policy and Institutional Issues."

[240] Ibid.

[241] "How Autonomous Vehicles Will Shape the Future of Surface Transportation."

[242] Ibid.

Many challenges will have to be overcome for successful deployment on a mass scale of connected and autonomous vehicle technology. Estimates indicate that the highest levels of autonomy, where drivers are relieved of some or all responsibility for driving will take five to twenty years.[243] Two primary obstacles to safe, secure autonomous and connected vehicle use will require exhaustive discussion on a national level are discussed below.

1.   Protection of Communication Systems from Cyber Attack

Protection of the communications systems that connected and autonomous vehicles will rely on is critical to public acceptance of this emerging technology. NHTSA has begun cyber security research, but recognizes that the work is dependent on available funding and will take three to four years.[244] Specifically NHTSA seeks to address the security of the control systems and how resistant the system will be from cyber attack while measuring risk by identifying gaps in the system that are subject to compromise.[245] In addition, NHTSA seeks to gauge how performance of the security system will impact operations of autonomous vehicles and most importantly what method can be identified to ensure critical subsystems are secure.[246]

As noted in Chapter III, the key element of the proposed security is based on a public key infrastructure (PKI) concept.[247] The system will make use of digital certificates that are validated or revoked according to an asymmetrical key pairing.[248] Since communications will be broadcast over an unsecure network, the PKI allows data

---

[243] Anderson et al., *Autonomous Vehicle Technology: A Guide for Policymakers*."

[244] "U.S. Department of Transportation Releases Policy on Automated Vehicle Development."

[245] Ibid.

[246] Ibid.

[247] Kim et al., "An Approach to Communications Security for a Communications Data Delivery System for V2V/V2I Safety," 14.

[248] Ibid.

exchanges that are certified as trusted by an independent authority using matching keys within the system.[249] The method is similar in design to that used for mobile banking and other commercial applications. The PKI may become the standard for security in the system and will be designed to limit availability of hacking.

The potential for attacking the communication system could come in two basic forms.[250] The first is an attack on the user. This action could cause the driver to be misinformed resulting in a possible accident, or as previously discussed criminal scenarios suggest, rerouting the vehicle to a new destination to facilitate a crime.

The sending of false information to vehicles or personal devices can also lead to traffic crashes. A new study conducted at the Virginia Tech Transportation Institute found that distracted driving is a cause for concern.[251] The study entitled, "*The Impact of Hand-Held and Hands-Free Cell Phone Use on Driving Performance an Safety Critical Event Risk*," revealed "that engaging in visual manual subtasks (such as reaching for a phone, dialing and texting) associated with use of hand-held phones and other portable devices increased the risk of getting into a crash by three times."[252]

By flooding data to a phone an inexperienced driver may become more susceptible to distraction and lose focus on driving tasks. Falsified data about a vehicle's mechanical status or authorization to use connected services could lead to potential revocation of digital certificates that allow connectivity to function.[253]

---

[249] Ibid.

[250] Ibid., 6.

[251] "New VTTI Study Results Continue to Highlight the Dangers of Distracted Driving."

[252] Ibid.

[253] Kyusuk Han, Swapna Divya Potluri, and Kang G. Shin, "On Authentication in a Connected Vehicle: Secure Integration of Mobile Devices with Vehicular Networks," in *Cyber-Physical Systems (ICCPS), 2013 ACM/IEEE International Conference on* (IEEE, 2013), 160–69, http://ieeexplore.ieee. org/xpls/abs_all.jsp?arnumber=6604010; Kim et al., "An Approach to Communications Security for a Communications Data Delivery System for V2V/V2I Safety: Technical Description and Identification of Policy and Institutional Issues."

The second form would be to attack the system itself through the use of denial of service attacks and jamming of wireless signals so that vehicles could not send or receive information.[254] As a result, vehicles would not function properly in autonomous mode or benefit from connected services. Successful attacks in either case would erode users' faith in the system and allow for expansion of criminal activity from cyber intrusion.

The key to security in any electronic system is to include hardware circuitry for security in the design phase with every computer control unit, which is not common in the automobile industry.[255] Integrity of software, data, communications, and access control to the system are critical to prevention of cyber attacks. The Society of Automotive Engineers (SAE) is currently engaged in the establishment of the J3061 Standard, *Cybersecurity Guidebook for Cyber-Physical Systems*, this guidebook addresses cybersecurity threats and will identify minimum standards as guidance to secure vehicle systems from cyber based attacks.[256] These standards will need to balance safety with privacy concerns for the protection of personal identifying information.

Costs of the security system have yet to be determined and may initially be exorbitant resulting in costs exceeding the projected figures for autonomous and connected vehicles. Experts in the automobile industry and DOT will have difficulty fixing costs as dynamic factors like production schedules and demand are uncertain. The security framework structure is under study but is considered a projection at best.[257]

---

[254] Kim et al., "An Approach to Communications Security for a Communications Data Delivery System for V2V/V2I Safety: Technical Description and Identification of Policy and Institutional Issues."

[255] Ibid., 16.

[256] "J3061 (WIP) Cybersecurity Guidebook for Cyber-Physical Automotive Systems," accessed October 3, 2015, http://standards.sae.org/wip/j3061/.

[257] United States Government Accountability Office, *Intelligent Transportation Systems: Vehicle-to-Vehicle Technologies Expected to Offer Safety Benefits, but a Variety of Deployment Challenges Exist* (GAO-14-13) (Washington, DC: U.S. Government Accountability Office, 2013), http://www.gao.gov/products/GAO-14-13.

2. Societal Considerations

Society has a vested interest in the development of this technology as privacy principles are intertwined with and must be balanced by the need for public safety. Recent revelations of mass data collection by government agencies have caused a surge in interest by the general public, as well as governmental leaders.

The 2014 Supreme Court's unanimous ruling in Riley vs. California that police need a search warrant prior to searching a cell phone signaled a clear message that digital information incorporates much more than simple data extraction and is to be handled differently. It is linked to every facet of an individual's life and exposure is more invasive thus individuals have a greater expectation of privacy. Access to mass data on individuals now requires greater scrutiny by judicial officials.[258] In a USA today article dated July 21, 2014 Chief Justice Roberts stopped short of expanding this case to other data inspection scenarios when he stated that the cell phone cases, "do not implicate the question whether the collection or inspection of aggregated digital information amounts to a search under other circumstances."[259]

Future research will help determine where the balance lies between what the public is willing to cede regarding their private information and the need for safety and security. The International Association of Chiefs of Police technology policy framework states, "creating and enforcing agency policies that govern the deployment and use of technology, protecting the civil rights and civil liberties of individuals, as well as the privacy protections afforded to the data collected, stored, and used, is essential to ensure effective and sustainable implementation, and to maintain community trust."[260]

Another key societal factor is understanding how humans will interact with this new technology. Understanding how and under what conditions humans will turn over

---

[258] "Riley v. California," accessed October 3, 2015, http://www.scotusblog.com/case-files/cases/riley-v-california/.

[259] Richard Wolf, "Justices' Cellphone Privacy Ruling May Have Broad Impact," *USA Today*, July 20, 2014, http://www.usatoday.com/story/news/nation/2014/07/20/supreme-court-cellphone-privacy-nsa-terrorism/12779997/.

[260] "Technology Policy Framework," accessed July 30, 2014, http://www.theiacp.org/ViewResult?SearchID=2361.

control of the vehicle to the onboard computer systems and more importantly how they can take back control when faults are detected has yet to be fully defined.

Legislation like the legal definition of driver will no doubt need to be substantially changed and will require adaptation by the legal community and law enforcement as well.[261] Currently, such activities as drinking and texting while driving are banned. With the introduction of high levels of automation, these prohibitions may no longer be necessary. Every duty that is placed by statute upon a driver will need to be evaluated for modification, even an operators' license may become obsolete.

A thorough review of the various governmental responses is necessary as the technology is introduced and becomes available to the consumer. An examination of key regulatory, legislative, and operational themes at the federal level will now be undertaken.

D.   FEDERAL REGULATORY GUIDANCE

Interestingly, regulatory guidance from the federal level is remarkably different for vehicles that have autonomous functionality compared to systems used for connected vehicle technology. Little guidance has been issued regarding autonomy, which is being met with approval from car manufacturers.

However, the federal government is extremely involved in the emergence of a connected vehicle system. Regulation is important to set standards for definitions and taxonomy, as well as ensuring public safety.

The Department of Transportation (DOT) was created by congressional action in 1966 and began operations in April 1967.[262] The agencies mission "is to ensure safe, efficient, accessible and convenient transportation systems that meet vital national interests while enhancing quality of life needs of Americans."[263] There are a number of agencies represented within DOT that issue regulations for various transportation

---

[261] Frank Douma and Sarah Aue Palodichuk, "Criminal Liability Issues Created by Autonomous Vehicles," *Santa Clara Law Review* 52, no. 4 (December 13, 2012): 1157.

[262] "About Us," March 1, 2012, http://www.dot.gov/mission/about-us.

[263] Ibid.

sectors.[264] Those entities that are specific to ground transportation systems that will regulate and issue rulemakings regarding autonomous and connected vehicles include:

- Federal Highway Administration (FHWA)

- Federal Motor Carrier Safety Administration (FMCSA)

- National Highway Traffic Safety Administration (NHTSA)

1. Automated Vehicles

NHTSA's preliminary guidance to the states was issued on May 30, 2013. The central theme of the document focused on safety.[265] The agency is responsible for "developing, setting, and enforcing Federal motor vehicle safety standards and regulations for motor vehicles and motor vehicle equipment."[266] Their safety programs seek to reduce crashes and injuries or deaths that result from crashes.

The statement focuses on the safety potential of autonomous vehicles and describes developments in automated driving and NHTSA's automated research program. The statement also offers preliminary guidance to states on testing and licensing, and clearly defines five levels of automation.[267]

> **Level 0:** No automation: The human driver is in complete control of all functions of the car."[268]
>
> **Level 1:** Function specific automation: One or more systems are automated for example cruise control, automatic braking, and lane keeping. Functions at this level operate independent of one another thereby ensuring the operator remains in physical control at all times.[269]
>
> **Level 2:** Combined function automation: More than one function is automated at the same time (e.g., steering and acceleration), but the driver

---

[264] "Regulatory Responsibilities and Contacts," accessed August 24, 2015, http://www.dot.gov/regulations/regulatory-responsibilities-contacts.

[265] "U.S. Department of Transportation Releases Policy on Automated Vehicle Development," 1.

[266] "U.S. Department of Transportation Releases Policy on Automated Vehicle Development," 1.

[267] Ibid., 4–5.

[268] "U.S. Department of Transportation Releases Policy on Automated Vehicle Development."

[269] Ibid.

must remain constantly attentive."[270] The driver is expected to be available for control at a moment's notice. Level 2 operations allow the driver to cede physical control for steering and acceleration/ braking in limited driving scenarios.

Level 3: Limited self-driving automation: The driving functions are sufficiently automated that the driver can safely engage in other activities."[271] Safety critical functions are handled by the automation features, but drivers will have sufficient transition time back to normal operating mode in the event the system determines it no longer can support the autonomous mode.

Level 4: Full self-driving automation: The car can drive and perform all safety-critical functions without aid from a human driver. Users will input destination or navigation information into the system but are not expected to assume control at any point.[272]

There is another important classification of levels of automation offered by the Society of Automotive Engineers International (SAE). The SAE, while not a federal government agency, provides technical specifications and standards for transportation sectors.[273] The federal government closely follows and is influenced by SAE recommendations as they are professionally generated by engineers, are highly technical, and establish best practices for industry.

One such standard is SAE J3016, *Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems*.[274] This standard provides a lexicon for levels of automation, which differ slightly from the NHTSA classifications. The SAE standard provides six levels of automation while NHTSA provides five.

---

[270] Ibid.

[271] Ibid.

[272] Ibid.

[273] "About," accessed August 26, 2015, http://www.sae.org/about/.

[274] "J3016: Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems," accessed October 16, 2014, http://standards.sae.org/j3016_201401/.

Figure 5.   SAE Levels of Automation

Summary of Levels of Driving Automation for On-Road Vehicles

This table summarizes SAE International's levels of *driving* automation for on-road vehicles. Information Report J3016 provides full definitions for these levels and for the italicized terms used therein. The levels are descriptive rather than normative and technical rather than legal. Elements indicate minimum rather than maximum capabilities for each level. "System" refers to the driver assistance system, combination of driver assistance systems, or *automated driving system*, as appropriate.

The table also shows how SAE's levels definitively correspond to those developed by the Germany Federal Highway Research Institute (BASt) and approximately correspond to those described by the US National Highway Traffic Safety Administration (NHTSA) in its "Preliminary Statement of Policy Concerning Automated Vehicles" of May 30, 2013.

Level	Name	Narrative definition	Execution of steering and acceleration/ deceleration	Monitoring of driving environment	Fallback performance of *dynamic driving task*	System capability (*driving modes*)	BASt level	NHTSA level
Human driver monitors the driving environment								
0	No Automation	the full-time performance by the *human driver* of all aspects of the *dynamic driving task*, even when enhanced by warning or intervention systems	Human driver	Human driver	Human driver	n/a	Driver only	0
1	Driver Assistance	the *driving mode*-specific execution by a driver assistance system of either steering or acceleration/deceleration using information about the driving environment and with the expectation that the *human driver* perform all remaining aspects of the *dynamic driving task*	Human driver and system	Human driver	Human driver	Some driving modes	Assisted	1
2	Partial Automation	the *driving mode*-specific execution by one or more driver assistance systems of both steering and acceleration/deceleration using information about the driving environment and with the expectation that the *human driver* perform all remaining aspects of the *dynamic driving task*	System	Human driver	Human driver	Some driving modes	Partially automated	2
Automated driving system ("system") monitors the driving environment								
3	Conditional Automation	the *driving mode*-specific performance by an *automated driving system* of all aspects of the *dynamic driving task* with the expectation that the *human driver* will respond appropriately to a *request to intervene*	System	System	Human driver	Some driving modes	Highly automated	3
4	High Automation	the *driving mode*-specific performance by an *automated driving system* of all aspects of the *dynamic driving task*, even if a *human driver* does not respond appropriately to a *request to intervene*	System	System	System	Some driving modes	Fully automated	3/4
5	Full Automation	the full-time performance by an *automated driving system* of all aspects of the *dynamic driving task* under all roadway and environmental conditions that can be managed by a *human driver*	System	System	System	All driving modes		

Today's technology advancements so far have reached level 1 (adaptive cruise control, forward collision avoidance, and lane departure warning), and limited level 2 status. Intelligent parking assist which allows hands free parallel or back-in parking in Toyota Prius vehicles is one example currently marketed and in operation in the United States.[275] Testing is on-going at the higher levels of automation and demonstrations have occurred recently to highlight the advancements of this technology.

2. Connected Vehicle Technology

The U.S. DOT is heavily involved in the regulation of connected vehicle technology. The Intelligent Transportation Systems Joint Program Office is instrumental in the development and deployment of the technical aspects of a connected transportation system.

The U.S. DOT has identified issues that will have an impact on successful deployment of a connected vehicle system. They include analysis and options for financial and investment strategies to cover the costs of implementing this vast system, which must be scalable to the entire country.

Comparisons of various communications platforms are currently underway to determine what type of service offers the best data delivery with low latency required for safety critical system performance. A key issue yet to be resolved centers around finalizing the structure of governance for the systems and what responsibilities will be assigned as this complex system is implemented. It is unknown currently if government will exclusively control operations or cede it to a private entity or a public-private entity. Some legal questions also remain unresolved like liability, privacy considerations, and policy on data ownership in a connected environment.[276]

---

[275] "All-New Third Generation Toyota Prius Raises the Bar for Hybrid Vehicles—Again," accessed July 23, 2014, http://toyotanews.pressroom.toyota.com/article_display.cfm?article_id=1759.

[276] "ITS ePrimer: Module 13," accessed August 24, 2015, https://www.pcb.its.dot.gov/eprimer/module13.aspx.

In addition to these concerns lies the larger issue of funding. It is of paramount importance to the research and development of autonomous and connected vehicles.[277] In addition to funding for the vehicle technology, funding for a highly robust and functional highway infrastructure system is required for the technology to operate at peak performance. These vehicles rely heavily on uniform standards for signage and lane markings.[278] The highways must be clearly and consistently marked to allow onboard systems to identify roadways, intersections, and related infrastructure to facilitate safe movement.[279]

Two key federal funding programs directly related to highway infrastructure are the Moving Ahead for Progress in the 21st Century (MAP-21), and the Highway Trust Fund (HTF). The MAP-21 fund became law in July 2012 providing funding for surface transportation programs. During the fiscal year (FY) 2013–2014 over 100 billion dollars was appropriated.[280]

The MAP-21 act improves safety by establishing performance goals by finding highway improvement projects, reducing congestion, and improving traffic flow efficiency while protecting environmental concerns.[281] MAP-21 also funds the Highway Safety Improvement Program responsible for infrastructure safety and fatality reduction programs. MAP-21 provides funding for "research and technology development in areas like highway safety, infrastructure improvement, planning and environment, highway operations, and exploratory advanced research."[282]

---

[277] "News Release," accessed October 3, 2015, http://www.aashtojournal.org/Pages/NewsRelease Detail.aspx?NewsReleaseID=1397.

[278] "Road Markings for Machine Vision," accessed October 3, 2015, http://apps.trb.org/cmsfeed/TRB NetProjectDisplay.asp?ProjectID=4004.

[279] Ibid.

[280] "MAP-21," accessed July 11, 2014, http://www.fhwa.dot.gov/map21/.

[281] "A Summary of Highway Provisions—MAP-21—Moving Ahead for Progress in the 21st Century," accessed July 16, 2014, http://www.fhwa.dot.gov/map21/summaryinfo.cfm.

[282] Ibid.

The Highway Trust Fund (HTF) consists of the highway account, which funds improvements and related transportation programs.[283] A major source of funding for the HTF derives from federal motor fuel taxes. The fund is also facing serious solvency issues.[284]

A journal report from the American Association of State Highway and Transportation Officials (AASHTO) dated February 2015 indicated that funds available from the HTF have declined over several years.[285] This reduced funding and uncertainty of future funding levels has created a trickledown effect as state transportation officials must scale back or cancel needed improvements, as they cannot count on federal funding to arrive.[286]

The Congressional Budget Office projected that Congress would need 85–90 billion dollars to cover projected shortfalls for a six-year reauthorization that would extend the HTF to May 2021.[287] President Obama has approved multiple extensions with the current extension of the HTF approved through November 2015.[288] Congress has yet to present a bill for presidential signature on the reauthorization of the fund and it is expected to be debated fully during the fall 2015 session.

Without needed funding the nation's transportation infrastructure will continue to degrade. The optical sensors and related equipment onboard connected vehicles rely upon infrastructure improvements across the United States. Many research programs that will enhance and create new technologies related to connected vehicle systems are also

[283] "A Summary of Highway Provisions—MAP-21—Moving Ahead for Progress in the 21st Century."

[284] Carol Wolf, "U.S. Highway Trust Fund Faces Insolvency Next Year, CBO Says," *Bloomberg*, January 31, 2012, http://www.bloomberg.com/news/2012-01-31/u-s-highway-trust-fund-faces-insolvency-next-year-cbo-says.html.

[285] "Reports Highlight Weakened Federal, State Investment in Roads, Transit Systems."

[286] "Wright Takes States' Case to Capitol Hill as Time Nears for Decisions on Trust Fund."

[287] "CBO Says Trust Fund Will Need $85–90 Billion in Added Revenue for Bill Running to June 2021," accessed June 5, 2015, http://www.aashtojournal.org/Pages/060515CBOestimate.aspx.

[288] "Trust Fund Advocates Press Congress During Recess to Soon Finish Long-Term Bill," accessed August 10, 2015, http://www.aashtojournal.org/Pages/080715congress.aspx; "Short-Term Highway Trust Fund Extensions Complicate Planning for States," accessed November 30, 2015, http://www.routefifty.com/2015/11/highway-trust-fund-extensions-planning-state-governments/123307/.

funded through these programs. If budgetary issues are not resolved to provide long term funding for MAP-21 and the HTF then research and development will be slowed pushing back the potential dates for deployment of self-driving and connected motor vehicles.

E.   STATE

There are only four states (Nevada, Florida, California, Michigan), and the District of Columbia that have authorized the testing/operation of autonomous vehicles.[289] It is unclear if specific legislative authority is even required to permit testing.[290] All of the enacted measures define an autonomous vehicle similarly, as vehicles capable of operations without human intervention.[291] The statutes generally designate the operator as the party activating the technology.[292]

This definition will require further modification as issues of determining who is a liable (driver, manufacturer, third party) involving crash or injuries will require identification in criminal and civil proceedings unless current jurisprudence practices likewise change.[293]

It is important to note the associated problems that could arise from regulating legislation from multiple states. Manufacturers would have difficulty marketing vehicles if different sets of standards were adopted by the states. Variances in state laws may hinder owners of autonomous vehicles as well if licensing authorities require operator endorsements that are not standardized. A national level framework for standardization will aid manufacturers, consumers, and public safety officials alike.[294]

The limited guidance issued to states by NHTSA on autonomous vehicles deals specifically with licensing and registration. NHTSA's function is related to safety

---

[289] Anderson et al., *Autonomous Vehicle Technology: A Guide for Policymakers*.

[290] Bryant Walker Smith, *Automated Vehicles Are Probably Legal in The United States* (Stanford, CA: The Center for Internet and Society (CIS) at Stanford Law School, 2012), http://cyberlaw.stanford.edu/ publications/automated-vehicles-are-probably-legal-united-states.

[291] Anderson et al., *Autonomous Vehicle Technology: A Guide for Policymakers*.

[292] Ibid.

[293] Douma and Palodichuk, "Criminal Liability Issues Created by Autonomous-Vehicles," 1158.

[294] Anderson et al., *Autonomous Vehicle Technology: A Guide for Policymakers*.

standardization and not homeland security. No guidance to date has been issued by any component of the Department of Homeland Security (DHS), nor the Federal Bureau of Investigation to prepare states for security plan development specific to this technology.

Additionally, NHTSA's policy statement outlines limited guidance to the states to help implement the technology safely. NHTSA was concerned about detailed state regulation of autonomous vehicles and noted that the issued guidance was provisional and subject to revision.[295] They further recognized that any state regulatory action must be balanced between ensuring motor vehicle safety and allowing innovation by industry.[296]

As for connected vehicle technology at the state level, there are no regulatory actions underway and the process is wholly within the realm of the federal government. Funding concerns for required infrastructure improvements as previously mentioned remain the major concern for state level transportation departments.

F.   VIRGINIA

There has been limited action in the Commonwealth of Virginia regarding autonomous vehicles. An initial joint agency meeting to discuss autonomous vehicles was conducted in Richmond, Virginia on October 29, 2013.[297] The stakeholders in attendance were the Virginia Department of Motor Vehicles, Virginia State Police, Virginia Department of Transportation, Virginia Center for Transportation Innovation and Research (VCTIR), and the Virginia Tech Transportation Institute. The study of autonomous vehicles is a continuation of the Non-Conventional Vehicles Study currently in progress. The consensus of the group was that Virginia should be in a posture to support autonomous vehicle testing without becoming overly restrictive. A permitting process was also recommended to review and approve autonomous vehicles for testing on public highways. No legislation was proposed for the 2014 or 2015 session of the General Assembly.

---

[295] "U.S. Department of Transportation Releases Policy on Automated Vehicle Development."

[296] Ibid., 10.

[297] Virginia State Police, meeting minutes and notes from author, July 8, 2014.

The Virginia Tech Transportation Institute demonstrated their autonomous vehicles during October 2015 using the express lanes on Interstate 95 and Interstate 395.[298] Executives from the U.S. Department of Transportation and congressional staff along with other stakeholders attended and participated in the demonstration, which was conducted on a 10 mile stretch of the interstate between the Pentagon and the Franconia-Springfield Parkway. The demonstration was intended to raise awareness for Congressional members and DOT officials to foster further research and development.

There were no state recommendations offered or discussion initiated regarding potential security concerns for this technology. While it is important that regulation move forward slowly to encourage the technology's development, as recommended by NHTSA, it is equally important that regulation include security measures to address potential criminal and homeland security issues.

1.   Role of Law Enforcement—Operations

The impact of autonomous and connected vehicles on transportation in America will also affect the operations of law enforcement. Motor vehicles transformed the country in the early 20th century when Henry Ford released his Model T in 1908.[299] He not only revolutionized the production assembly line process but his work sparked efforts on a national level to spur road development.[300] Interestingly enough the Federal Bureau of Investigation was also created the same year by Attorney General Charles Bonaparte.[301]

It did not take long before vehicles became a platform for enhancing criminal activity. The Mann (White Slave) Act was passed in June 1910 making the interstate

---

[298] "Virginia Tech Transportation Institute, Partners Test Automated, Connected Vehicles on Interstate," accessed November 30, 2015, http://www.vtnews.vt.edu/articles/2015/10/101915-vtti-researchtest.html.

[299] Ada Lio, "History of American Roads and the First Federal Highway," About.com Inventors, accessed August 27, 2015, http://inventors.about.com/library/inventors/blcar3.htm.

[300] Ibid.

[301] "Brief History of the FBI," accessed August 27, 2015, https://www.fbi.gov/about-us/history/brief-history/brief-history.

transportation of women for immoral purposes illegal.[302] The automobile played a central role in interstate crime by allowing criminals to take advantage of the mobility offered by vehicles. As vehicles became more robust and ubiquitous in society, law enforcement adapted its role to fight crimes that were facilitated with the use of vehicles while at the same time making use of the technology to aid in the public safety mission. The same evolution will be required in the near future as autonomy is introduced to the consumer.

The traditional traffic enforcement role of state and local police departments across the country will undergo change as autonomous and connected vehicles become more prevalent. Agencies are responsible for ensuring safe, efficient traffic flow and traffic enforcement is one mechanism for achieving that goal.

Some have suggested that significant reductions in violator contacts will occur since autonomous vehicles obey all traffic laws and humans are removed from the decision making process.[303] However, this argument can be countered by the fact that motor vehicle equipment like tires, lights, exhaust, windshields, brakes all degrade with normal wear and tear. If routine maintenance is not performed equipment violations will become evident giving rise to reasonable suspicion thereby allowing interactions with law enforcement.

As an example, the Virginia State Police is mandated to implement the state's vehicle inspection program.[304] All Virginia registered motor vehicles, trailers, and semitrailers are subject to an annual inspection unless specifically exempted.[305] During 2014 licensed safety inspectors conducted 7,902,389 million vehicle safety inspections and identified 1,378,257 million vehicles with defects serious enough to warrant rejection

---

[302] "Brief History of the FBI."

[303] Sarah Aue Palodichuk, "Driving into the Digital Age: How SDVs Will Change the Law and Its Enforcement," *Minn. JL Sci. & Tech.* 16 (2015): 827–1011.

[304] "Virginia Administrative Code—Title 19. Public Safety—Agency 30. Department of State Police Agency Summary," accessed August 28, 2015, http://law.lis.virginia.gov/admincode/title19/agency30/preface/.

[305] "§ 46.2-1157. Inspection of Motor Vehicles Required," 2, accessed August 28, 2015, http://law.lis.virginia.gov/vacode/title46.2/chapter10/section46.2-1157/.

for unsafe components.[306] The percentage of rejection for all vehicles submitted was 17.4 percent.[307] There is ample evidence in these statistics to show that nearly one fifth of the vehicles on the roadway contain serious equipment violations.

Similar data is reported by the Federal Motor Carrier Safety Administration (FMCSA). The agency conducts safety inspections of motor carriers and can place the vehicle Out of Service (OOS) for violations of federal code related to equipment violations. The FMCSA's Motor Carrier Safety Progress Report as of March 31, 2015 indicates an OOS rate for roadside inspection of large trucks at 20.5 percent for the period October 2014 to March 2015.[308]

Clearly, the maintenance of vehicles is an issue that will not be resolved by autonomy. Equipment degradation and maintenance standards for private and commercial vehicles will remain an issue requiring law enforcement interaction with motorists and is a viable public safety concern.

Rules of the road are also likely to require change with autonomy, as autonomous and connected vehicles will operate with precision on the highway. They will be computer controlled and are designed to follow specific pathways calculated by their on-board optical sensors and mapping software previously installed.

Vehicles will communicate constantly with other vehicles and infrastructure in proximity and as a result precise movement of traffic is predictable. Current highways and streets are built with sufficient width to allow not only for the physical dimensions of the various vehicles using the roadways, but safety margin allowances are made for the human equation of imprecise driving behaviors.[309] With the introduction of autonomy in vehicle systems roadways throughout the nation may be altered to reduce lane width

---

[306] Virginia State Police, *Facts and Figures Report 2013* (Richmond, VA: Virginia State Police, 2014), http://www.vsp.state.va.us/Annual_Report.shtm.

[307] Ibid.

[308] "Motor Carrier Safety Progress Report (as of March 31, 2015)," accessed August 28, 2015, http://www.fmcsa.dot.gov/safety/data-and-statistics/motor-carrier-safety-progress-report-march-31-2015.

[309] "A Policy on Geometric Design of Highways and Streets 2001," 15, 2001, http://nacto.org/docs/usdg/geometric_design_highways_and_streets_aashto.pdf.

requirements as new highway construction and maintenance projects are initiated or updated.[310]

2.   Legislation

Autonomous vehicles with connected technology will transform the ground transportation system, but will also require careful consideration and adaptation of existing statutory law in the areas of insurance, traffic, and criminal codes. Legislators at all levels of government will have to consider and address questions of legality and criminal conduct involving operation of these vehicles on public highways. Insurance and liability concerns will need to be clarified to satisfy market demands. Requirements for operator responsibilities will need to be answered, and data and privacy issues related to transmission and ownership of data shared between vehicles and the infrastructure will have to be solidified. These areas continue to evolve so policy decisions will be difficult to construct and implement all at one time.

The policy guidance issued by NHTSA in 2013 recommended that states refrain from enacting specific safety regulations to prevent stifling innovation in this rapidly changing field.[311] However, potential legislation likely will be crafted based on this guidance so a brief overview is warranted.

Technology development often exceeds the capacity of governments to keep pace with regulation. NHTSA instead has recommended that states focus on specific objectives related to testing operations for self-driving cars in the following categories:

- Licensing drivers to operate Self-Driving Vehicles (SDVs) for testing

- Issue state regulations governing testing of SD's

- Establish basic principles for testing of SD's

- Issue regulations governing operation of SDVs for purposes other than testing[312]

---

[310] Smith, "Managing Autonomous Transportation Demand," 1401.

[311] NHTSA, *2013 Traffic Safety Facts DOT* (Washington, DC: National Highway Traffic Safety Administration, 2013), http://www-nrd.nhtsa.dot.gov/Pubs/812139.pdf.

[312] "U.S. Department of Transportation Releases Policy on Automated Vehicle Development."

These categories contain guidance that ensures states develop training programs to assist drivers in understanding how to operate an autonomous vehicle safely while minimizing risks to other vehicles during testing. Another consideration was for states to ensure that testing areas are limited in terms of highway type or geographical location to maximize safety. The ability for the state to capture potential crash data for any vehicle involved in testing was also recommended to build on the data available for future research. The state of California enacted that specific requirement in its legislation enabling it to document instances of crashes involving Google's fleet of autonomous vehicles.[313]

Guidance specific to how the technology interacts with the operator, also known as Driver Vehicle Interface (DVI) was also recommended. States were cautioned to ensure the processes for the interaction between the operator and vehicle were "safe, simple, and timely," and that test vehicles could detect, record, and alert the operator of malfunctions in the system.[314]

A final caution to states concerns maintaining oversight to ensure federally required safety features and systems are not disabled. Federal law prohibits manufacturers, dealers, and motor vehicle repair facilities from disconnecting required systems.[315]

3. Liability

The issue of liability will likewise require clarification as SDVs are introduced into the marketplace. Determining who or what entity could be responsible for a crash and/or personal injury accident will be established by legislative authority, but potentially altered by judicial case law as litigation weaves its way through the court systems around the globe. The passage of legislation will no doubt have an effect on the deployment of the technology as manufactures, software engineers who write the computer code for

---

[313] "First Set of Autonomous Vehicle Regulations Are Now in Effect," accessed August 28, 2015, https://www.dmv.ca.gov/portal/dmv/detail/pubs/newsrel/newsrel14/2014_61a.

[314] "U.S. Department of Transportation Releases Policy on Automated Vehicle Development."

[315] Ibid.

algorithms, and after-market equipment installers will want to have reasonable assurances of where liability will fall in the event of litigation arising from an incident involving the technology.[316]

Some legal experts suggest that current product liability law will adapt to autonomous vehicles similar to how the industry has handled issues surrounding the introduction of seat belts, air bags, and cruise control in the automotive marketplace.[317] It is understandable that manufacturers will be reluctant to release the full capacity of autonomy until liability concerns are addressed and stabilized with an appropriate structure solidified by judicial case law interpretation.[318]

To answer some of the product liability or negligence claims, courts will likely look to definitions in the statutes. Some of the intriguing definitions related to autonomous vehicle use that will require research and analysis include the terms driver, chauffer, operator, and user. While it is recognized that each state legislative body may have placed different language in their current definitions to describe these terms all should be re-evaluated in light of the capabilities of self-driving cars.

Currently, the Code of Virginia defines an operator or driver in Section 46.2-100 Definitions as:

> Operator or Driver means every person who either (i) drives or is in actual physical control of a motor vehicle on a highway or (ii) is exercising control over or steering a vehicle being towed by a motor vehicle.[319]

Similarly, the term chauffer is defined in the same section as:

---

[316] Roy Alan Cohen, "Self-Driving Technology and Autonomous Vehicles: A Whole New World for Potential Product Liability Discussion," *Defense Counsel Journal* 82, no. 3 (2015): 331.

[317] "'Look Ma, No Hands!' Wrinkles and Wrecks in the Age of Autonomous Vehicles," accessed August 27, 2014, http://newenglrev.com/volume-46-issue-3/v46b3garza/.

[318] Cohen, "Self-Driving Technology and Autonomous Vehicles," 331.

[319] "§ 46.2-100. Definitions," accessed August 28, 2015, http://law.lis.virginia.gov/vacode/title46.2/chapter1/section46.2-100/.

Chauffer means every person employed for the principal purpose of driving a motor vehicle and every person who drives a motor vehicle while in use as public or common carrier of persons or property.[320]

These two Virginia definitions illustrate the necessity for a modification of the statutory definitions. Current descriptions require a human to interact with the vehicle to manipulate control mechanisms. As upper levels of autonomy are introduced, a "driver" may be required on a limited basis or not at all. A new definition for "user" may actually offer a more descriptive term for an individual using an autonomous vehicle.

There are a number of statutes outlining moving infractions that will also require alteration as they impose a duty or responsibility upon a driver. For example, a driver involved in a motor vehicle crash is required to stop and give notice or else face possible prosecution for leaving the scene of an accident.

Drivers in some states, like Virginia, are also required to give notice to state officials of certain accidents involving personal injury, death or when property damage exceeds minimum reporting criteria.[321] Drivers in numerous states are also prohibited from certain actions while driving like texting or using cellular devices. The classification of driver will need to be revised to reflect a more accurate description of what an operator is allowed to do while at the same time establishing responsibility when the operator is riding in an autonomous vehicle.

As states debate and ultimately decide on specific language for definitional terms they must also consider the impacts that can be realized with full automation. As entire segments of society that were previously unlicensed for reasons of age, infirmity, or other physical impediment, (e.g., blindness) are able to take advantage of the mobility offered from autonomy the question to consider long term is whether licensing will even be required for future generations. How will future driver training programs be affected, and will there be a resultant degradation of driving skills for new users of autonomy?

---

[320] "§ 46.2-100. Definitions."

[321] "§ 46.2-372. Driver to Report Certain Accidents in Writing; Certification of Financial Responsibility to Department; Supplemental Reports; Reports by Witnesses," 2, accessed September 1, 2015, http://law.lis.virginia.gov/vacode/title46.2/chapter3/section46.2-372/.

If a driver's license, which currently serves as a legal document, and official form of government identification in addition to authorizing an individual to drive on the public highway were to become obsolete what would take its place to fill those requirements? Furthermore, an operator's license is subject to revocation or suspension by the issuing authority or the court for punitive sanction or administrative reasons. What mechanism would the courts or issuing authorities rely on to sanction individuals for violations of law or administrative violations and how would that system work to encourage compliance if licenses do not exist?

G.   CONCLUSION

The emergence of autonomous and connected vehicles will impact the entire ground transportation system. The possibility of unintended consequences is relevant and attention to detail should be given to the areas discussed in this chapter. These hard questions will need to be discussed in working groups that include the American Association of Motor Vehicle Administrators, Judges, law enforcement, and other judicial authorities with input from concerned stakeholder groups. The answers to some of the questions will be as fluid as the emergence of the technology itself.

The concern of many advocates of this technology is security of the involved systems. While structures have not been completely finalized, it is recognized that interconnected systems that operate wirelessly are subject to cyber intrusion. The following chapter will illustrate this major concern and discuss a project undertaken by the Virginia State Police and other stakeholders to begin to understand why these systems are vulnerable and offer a path forward for mitigation and protection of police vehicle fleets. The same vulnerabilities identified in this project will transfer to autonomous and connected vehicles and their related systems.

V.   THE CYBER NEXUS

It is becoming increasingly difficult to open any news site today without reading about cyber invasions, data breaches, and privacy compromises. No sector has gone unscathed. The size, scope, and expense of dealing with cybersecurity issues has been increasing in recent years with notable intrusions occurring in the private sector and most recently within the governmental sector as was the case with the Office of Personnel Management.[322] The burden and expense of these intrusions is borne by the victims and defenders who rely on a risk based methodology for protecting vital assets.

Recent revelations regarding cyber attacks on motor vehicles have been highlighted in media and have garnered the attention of Congressional members. Senator Edward Markey, D-Mass has complained loudly about the unwillingness of some automakers to have definitive discussions about the security of their products from cyber attack.[323]

The message has been conveyed in the private sector as well when a grassroots organization known as "I Am the Calvary" sent an open letter to automobile manufacturers in August 2014.[324] The intent of the letter was to encourage cooperation among manufacturers and the cyber security community and outlined five critical capabilities collectively known as the "5 Star Automotive Cyber Safety Program." The letter raised awareness and visibility of this emerging threat to transportation but more so for the lack of response by the auto industry.[325]

Cyber security is a new frontier that has demonstrated its impact on computer information systems via hacking. It is logical that networked systems and physical

---

[322] "Why The OPM Breach Is Such a Security and Privacy Debacle," June 11, 2015, http://www. wired.com/2015/06/opm-breach-security-privacy-debacle/.

[323] Andy Greenberg, "Hackers Could Take Control of Your Car. This Device Can Stop Them," *WIRED*, July 22, 2014, http://www.wired.com/2014/07/car-hacker/.

[324] "Five Star Automotive Safety Program," accessed February 5, 2015, https://www.iamthe cavalry.org/domains/automotive/5star/.

[325] Ibid.

systems, like cars, will be susceptible to cyber intrusion. Autonomous and connected vehicles fall squarely in this realm and their system of systems must be protected.

There is to date no method for recording data specific to cyber attacks on motor vehicles on a national basis. The analysis of data will be fundamental in establishing how pervasive the threat is to transportation, and will supply researchers with valuable information regarding attack methodology. This chapter will lay a foundation for correcting this deficiency.

The chapter will be segmented into four distinct parts. First the reader will be exposed to a generalized description of the current cyber security environment in the United States. Second will be a brief discussion of law enforcement's response to these crimes, followed by an analysis of cyber security vulnerabilities for automobiles. Lastly, this research will describe in detail a public- private partnership created in January 2015 in Virginia to examine vulnerabilities in Virginia State Police (VSP) cruisers currently operated by the agency. While autonomous and connected vehicles were not used during the VSP project a comparison can be made between current vulnerabilities and future attacks that are expected on those vehicles. An argument will be framed for development of forensic tools for analysis of cyber related incidents at the scene of any incident that law enforcement might suspect cyber activity.

A.   CURRENT SITUATION

On September 15, 2015, the Director of National Intelligence James R. Clapper, appearing before the House Permanent Select Committee on Intelligence stated that "cyber threats to the United States are increasing in frequency, scale, sophistication, and severity of impact.[326] Nearly all information communication technologies and information technology networks and systems have vulnerabilities and contain some level of risk."[327] Director Clapper did not envision a future catastrophic event involving cyber

---

[326] "DNI Clapper Statement for the Record, Worldwide Cyber Threats before the House Permanent Select Committee on Intelligence," accessed October 5, 2015, http://www.dni.gov/index.php/newsroom/testimonies/209-congressional-testimonies-2015/1251-dni-clapper-statement-for-the-record,-worldwide-cyber-threats-before-the-house-permanent-select-committee-on-intelligence.

[327] Ibid.

attack, but indicated, "an ongoing series of low-to-moderate level cyber attacks from a variety of sources over time which will impose cumulative costs on U.S. economic competitiveness and national security."[328]

Similarly, a Federal Times article dated September 23, 2015, outlines how pervasive cyber intrusions have become in the federal system.[329] The Energy Department (DoE) reported cybersecurity events over a 48 month period between fiscal year 2010 and fiscal year 2014 totaling 1,131 major cyber incidents.[330] These incidents ranged from intrusion assaults into DoE networks and user accounts, to malicious code installation, unauthorized network access, and attacks designed to prevent of slow daily operations.[331]

The Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) has responsibility for "improving the Nation's cybersecurity posture, coordinating cyber information sharing, and proactively managing cyber risks."[332] Federal agencies reported 5,503 cyber incidents to the US-CERT in 2006, but by 2014 reports dramatically increased 1,220 percent to 67,168 reported incidents.[333]

A September 2015 Government Accountability Office report GAO-15-714, entitled *Federal Information Security: Agencies Need to Correct Weaknesses and Fully Implement Security Programs* highlighted persistent cyber weaknesses in twenty-four federal agencies.[334] The identified areas noted in the report include:

- Limiting, preventing, and detecting inappropriate access to computer resources

---

[328] "DNI Clapper Statement for the Record, Worldwide Cyber Threats before the House Permanent Select Committee on Intelligence."

[329] "Government Operations, Agency Management, Pay & Benefits," accessed October 5, 2015, http://www.federaltimes.com/story/government/management/blog/2015/09/23/cyber-onslaught-gets-worse/72688016/.

[330] Ibid.

[331] Ibid.

[332] "About Us," accessed October 5, 2015, https://www.us-cert.gov/about-us.

[333] "Government Operations, Agency Management, Pay & Benefits."

[334] United States Government Accountability Office, *Federal Information Security: Agencies Need to Correct Weaknesses and Fully Implement Security Programs* (GAO-15-714) (Washington, DC: U.S. Government Accountability Office, 2015), http://www.gao.gov/products/GAO-15-714.

- Managing the configuration of software and hardware

- Segregating duties to ensure that a single individual does not control key aspects of computer-related operation

- Planning for continuity of operations

- Implementing agency-wide security management programs[335]

It is evident from the report that cyber security issues are not solely the result of failures in systems security but rather an integrated problem that human operators also contribute to as well.

B.   LAW ENFORCEMENT RESPONSE

Cyber intrusions are now becoming commonplace and personally identifiable information is immediately converted by criminal actors for profit.[336] Victims are unsure of how to respond to an attack, and law enforcement agencies struggle with attribution and prosecution due to limited technical expertise, crimes that extend beyond geographical borders, and complexity of attacks that traverse multiple servers and routers. This lax response helps contribute to a permissive environment that fosters more crime.

Identifying how, and under what circumstances, cyber attacks are promulgated is now a major concern for law enforcement. Developing methods, tactics, and procedures to deny attacks and mitigate damage to systems is emerging as a priority. Identifying attackers that target systems and bringing them to justice will require a multi-disciplinary approach. Police officers must gain investigatory knowledge in computer information systems, physical systems, and multi-jurisdictional case investigation procedures to effectively handle these complex investigations. Cyber criminals actively use the Internet

---

[335] United States Government Accountability Office, *Federal Information Security: Agencies Need to Correct Weaknesses and Fully Implement Security Programs*.

[336] "National Cyber Security Awareness Month," accessed October 5, 2015, https://www.fbi.gov/ news/stories/2015/october/national-cyber-security-awareness-month/national-cyber-security-awareness-month.

to facilitate crimes involving fraud, identity theft, financial schemes, and intrusion of computer systems to inject malware.[337]

The Department of Homeland Security (DHS) plays a pivotal role in cybersecurity by protecting the nation's critical infrastructure and ensuring law enforcement responses to cyber threats are adequate to meet emerging threats. With its global range and cross disciplinary structure the agency is positioned well to aid in cybersecurity defense both in a defensive capacity and through in depth research and development. However, more focus on employing all of the assets in the various components should be emphasized.[338] Its authority and creation is derived from The Homeland Security Act of 2002.[339] DHS also receives authority for cybersecurity operations from a number of Presidential Policy Directives (PPD-8, 21) and Executive Order 13636.[340] This agency also maintains a Cyber Division within the DHS Science and Technology Directorate that conducts research to support stakeholders across the nation.[341]

The Federal Bureau of Investigation (FBI) has taken a leading role in the investigation of cyber related crimes. The agency leads the National Cyber Joint Investigative Task Force, which serves as coordinating agency for cyber investigations. To respond to this threat each of the fifty-six field offices in the nation has agents assigned to this role.[342]

---

[337] "National Cyber Security Awareness Month."

[338] Edward W. Lowery, "Closing the Cyber Gap: Integrating Cross-Government Cyber Capabilities to Support the DHS Cyber Security Mission" (master's thesis, Naval Postgraduate School, 2014), 18–19, http://calhoun.nps.edu/handle/10945/44608.

[339] Sharon S. Gressle, *Homeland Security Act of 2002: Legislative History and Pagination Key* (CRS Report Order Code RL31645) (Washington, DC: Congressional Research Service, 2002), http://digital.library.unt.edu/ark:/67531/metacrs7490/m1/1/high_res_d/RL31645_2002Nov26.pdf.

[340] Department of Homeland Security, *Presidential Policy Directive 8: National Preparedness* (Washington, DC: Department of Homeland Security, 2011), http://www.dhs.gov/presidential-policy-directive-8-national-preparedness; "Presidential Policy Directive—Critical Infrastructure Security and Resilience," accessed December 1, 2015, https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil; "Executive Order 13636," accessed December 1, 2015, http://fas.org/irp/offdocs/eo/eo-13636.htm.

[341] "Cyber Security Division," accessed December 1, 2015, http://www.dhs.gov/science-and-technology/cyber-security-division.

[342] "National Cyber Security Awareness Month."

Infragard is a public-private partnership set up like an information sharing and analysis center where private companies partner with the FBI to identify and mitigate vulnerabilities, develop response plans, and create best practices to protect the nation's infrastructure.[343] The FBI also interacts with the community through the Internet Crime Complaint Center (IC3), and the Safe Online Surfing website. Both programs seek to inform and educate the public about cyber related issues.[344]

The International Association of Chiefs of Police (IACP) also actively trains the nation's officers in cyber related matters. The IACP released in September 2015 a Cyber Crime Checklist for Police Chiefs that offers a reference guide for understanding cyber issues complete with resource links to obtain additional information.[345] The agency has also enacted a cyber security framework to be used as a tool for establishing protections in operations, facilities, and policy related to cyber.[346]

While much planning and discussion has gone into how law enforcement agencies should protect their information systems like computing and dispatch centers, little has been advanced in regards to the protection of vehicle fleets. Patrol vehicles are the cornerstone for agencies to respond to calls for service from the citizenry. It is a logical step for police managers to give consideration to how vehicles might be cyber attacked.

C. CYBERSECURITY FOR AUTOMOBILES

Intelligent Transportation Systems (ITS) that are emerging around the globe achieve that classification based on the convergence of smart technologies that allow the included systems to communicate and share data in real time.[347] These systems rely on architectures that have varying degrees of security protocols embedded, which could lead to vulnerabilities internally and externally by cyber intrusion.

---

[343] "National Cyber Security Awareness Month."

[344] Ibid.

[345] "Chief's Checklist," accessed October 4, 2015, http://www.iacpcybercenter.org/chiefs/it-security/chiefs-checklist/.

[346] "Home," accessed October 5, 2015, http://www.iacpcybercenter.org/.

[347] "Fast Facts," accessed October 6, 2015, http://its.dot.gov/fastfacts.htm.

Autonomous and connected vehicles once were considered concepts for the future, but because of accelerated research and development, they are poised to enter the consumer market within the next decade. These vehicles are systems of systems and include hardware and software that enable communications and operations with little to no input from a human. The modern automobile contains numerous electronic control units (ECU's) that control information and functions within the car like brakes, lighting, and drivetrain components.[348] These ECU's will also be present in autonomous and connected vehicles and will function in similar manner to today's automobile.

The vehicle's ECU's are connected via electrical architecture in an internal network that routes data through a Controller Area Network (CAN) bus.[349] While this configuration provides reduced costs to manufactures, it does allow data to flow from individual system components through a central processing unit. However, this arrangement creates the possibility for serious consequences in the event of a cyber attack. Once access is gained to the CAN bus an attacker could manipulate individual safety critical functions in the car.[350]

This process would require the attacker to have knowledge of the vehicle's electrical system, and the data packets that signal and control individual systems to perform a specific function. This is achieved through experimentation by "fuzzing" where wireless signals are captured after observing data flows on a computer that is in proximity to the target vehicle.[351]

The attacker would then need access to the vehicle or have sufficient knowledge to execute a remote attack via an external attack surface like Bluetooth, cellular phone or

[348] Tobias Hoppe, Stefan Kiltz, and Jana Dittmann, "Security Threats to Automotive CAN networks—Practical Examples and Selected Short-Term Countermeasures," *Reliability Engineering & System Safety* 96, no. 1 (January 2011): 11, doi:10.1016/j.ress.2010.06.026.

[349] Stephen Checkoway et al., "Comprehensive Experimental Analyses of Automotive Attack Surfaces," in *USENIX Security Symposium*, 2011, http://static.usenix.org/events/sec11/tech/full_papers/ Checkoway.pdf.

[350] Karl Koscher et al., "Experimental Security Analysis of a Modern Automobile" (IEEE, 2010), 448, doi:10.1109/SP.2010.34.

[351] Ibid., 454.

infotainment systems in the car.[352] Most major car manufacturers now have Telematics, like GM's On Star as optional packages on their vehicles, which provide driver services, but also provide an attack surface into the vehicle.[353]

The remote attack is much more sophisticated but has recently been executed by two cyber researchers named Miller and Valasek.[354] An exhaustive discussion on remote attacks is also presented in a paper entitled, "*Comprehensive Experimental Analyses of Automotive Attack Surfaces*.[355]

Direct physical access to a vehicles internal network system can be achieved by multiple means. Methods include insertion of malware from a compact disk (CD) into the CD player or inserting an infected universal serial bus (USB) drive into a USB port. Connecting a digital media device (iPod/iPhone) or similar device with embedded malware would achieve the same result.

A vehicle's On Board Diagnostic (OBD) port is particularly vulnerable and easily accessed near the steering wheel beneath the dashboard. These OBD ports are federally mandated in the United States and are most often used by mechanics for diagnosis and programming of the ECU's on the vehicle.[356] This port provides access to the vehicles CAN buses from which access to automotive systems can be achieved with relative ease.[357]

It is not the intent of this paper to articulate specific attack scenarios or how to accomplish them, however it is critical to understand that autonomous and connected vehicles will have similar electrical CAN bus architecture as current vehicles and will be subject to similar attack by nefarious actors.[358]

---

[352] Checkoway et al., "Comprehensive Experimental Analyses of Automotive Attack Surfaces."

[353] Koscher et al., "Experimental Security Analysis of a Modern Automobile," 449.

[354] Greenberg, "Hackers Could Take Control of Your Car. This Device Can Stop Them."

[355] Checkoway et al., "Comprehensive Experimental Analyses of Automotive Attack Surfaces."

[356] "A Brief Intro to OBD-II Technology," accessed October 5, 2015, http://www.cnet.com/news/a-brief-intro-to-obd-ii-technology/.

[357] Checkoway et al., "Comprehensive Experimental Analyses of Automotive Attack Surfaces."

[358] Kim et al., "An Approach to Communications Security for a Communications Data Delivery System for V2V/V2I Safety: Technical Description and Identification of Policy and Institutional Issues."

Evidence suggests that vehicles could become a target for hackers, but the National Highway Traffic Safety Administration recently acknowledged a dearth of qualified engineers to research cyber related issues.[359] The Electronics Systems Safety Research Division has a total of seven employees in two locations. They are responsible for testing and evaluating cyber vulnerabilities among other assigned duties.[360]

NHTSA also intends to create a Cyber Information Sharing Analysis Center for vehicles.[361] Automakers agreed to the idea in July 2014 to allow for the exchange of information, but the center has yet to open. NHTSA officials are now concerned that future attacks on connected vehicles will have the potential to affect multiple cars in a single event.[362]

The U.S. Department of Homeland Security is also concerned about cyber security for motor vehicles. The DHS Science and Technology Directorate (DHS S&T), the Cyber Security Division, and the U.S. Department of Transportation Volpe Center (DOT Volpe), and the non-profit research institute SRI International have formed a new Government Vehicle Cybersecurity Steering Group that met in October 2015.[363] This group will assess the threat to government vehicles and develop appropriate security measures.

Law enforcement across the nation should be concerned with preparing for how to investigate cyber attacks on vehicles. They should be equally concerned with ensuring their own fleet vehicles are protected so that the public safety mission can still be achieved. It was this thought that drove the recent public-private partnership undertaken by the Virginia State Police.

---

[359] "Short-Staffed NHTSA Struggles to Handle Car-Hacking Threats," accessed October 5, 2015, http://www.autoblog.com/2015/10/02/short-staffed-nhtsa-struggles-to-handle-car-hacking-threats/.

[360] Ibid.

[361] Ibid.

[362] Ibid.

[363] Invitation in possession of author to participate in Government Vehicle Cybersecurity Steering Group Kickoff Meeting, October 22, 2015. Dr. Dan Massey, DHS, e-mail message to the author, September 15, 2015.

D. VIRGINIA STATE POLICE CYBER SECURITY PROJECT

During the month of January 2015, Dr. Barry Horowitz, Munster Professor of Systems and Information Engineering at the University of Virginia (UVA) contacted the Virginia State Police regarding a proposal for cyber security for the agencies vehicles. Dr. Horowitz has significant experience in cyber security and has focused his research on embedding security solutions into systems. As the project became solidified and partners were added to the project team the Governor of Virginia made two relevant announcements with respect to this effort.

On April 20, 2015, Governor Terry McAuliffe announced that the Commonwealth of Virginia would create an Information Sharing Analysis Organization (ISAO).[364] This statement followed President Obama's issuance of Executive Order 13691 *Promoting Private Sector Cybersecurity Information Sharing,* directing DHS to encourage ISAO's across the nation.[365] The Virginia ISAO will share cyber threat information across government and industry sectors.[366] It is anticipated that the VSP project details will be shared with this organization.

On May 15, 2015, Governor McAuliffe announced the establishment of a public-private partnership with the Virginia State Police to "explore the technology needed to safeguard Virginia's citizens and public safety agencies from cybersecurity attacks targeting automobiles."[367]

This effort would receive coordination from the U.S. Department of Homeland Security's Science and Technology Directorate and the U.S. Department of Transportation's Volpe National Transportation Systems Center.[368] The other parties to the partnership include the Virginia Department of Motor Vehicles, University of

---

[364] "Governor McAuliffe Announces State Action to Protect against Cybersecurity Threats," April 20, 2015, http://governor.virginia.gov/newsroom/newsarticle?articleId=8210.

[365] "Executive Order 13691," accessed October 6, 2015, http://fas.org/irp/offdocs/eo/eo-13691.htm.

[366] "Governor McAuliffe Announces State Action to Protect against Cybersecurity Threats."

[367] "Governor McAuliffe Announces Initiative to Protect against Cybersecurity Threats," May 15, 2015, http://governor.virginia.gov/newsroom/newsarticle?articleId=8430.

[368] Ibid.

Virginia, The MITRE Corporation, and private-sector cybersecurity companies including Mission Secure, Inc., Spectrum Comm., Kaprica Security, and Digital Bond Labs.[369] Two additional partners were added after the official announcement and contributed to the project. They were the Aerospace Corporation and The Applied Physics Lab at John Hopkins University.

The following goals were established for the work group to aid in the protection of Virginian's vehicles and those operated by law enforcement.

- Identify low-cost technology that can be developed to assist law enforcement officers and investigators in determining if/when a vehicle or other mechanized equipment has fallen victim to a cyber attack.

- Develop strategies for Virginia citizens and public safety personnel to identify and prevent cybersecurity threats targeting vehicles and other consumer devices.

- Explore the economic development opportunities related to this specialized cybersecurity field within the Commonwealth.[370]

With the rapid advancement of the Internet of Things (IOT) technologies systems are more and more reliant upon electronic wireless communications. But little investment has occurred in security protections as these systems advance.

Dr. Horowitz proposed testing the VSP fleet to determine if agency vehicles were vulnerable to cyber attack, and if so, what attack vectors would be used. Additionally, possible detection and mitigation processes, along with forensic capability were proposed to ensure the integrity of the fleet and aid in the investigatory process following an attack. The proposed project was anticipated to last for 90 days. There was no funding for the project and companies agreed to bear any associated costs.

UVA has created a System-Aware Cybersecurity concept that is added as a layer of protection for physical system control functions.[371] The protection capability monitors

---

[369] "Governor McAuliffe Announces Initiative to Protect against Cybersecurity Threats."

[370] Ibid.

[371] "Security Engineering—Design Patterns and Operational Concepts," accessed October 6, 2015, http://www.sercuarc.org/research/research-program-and-projects/security-engineering-design-patterns-and-operational-concepts-tasks-28-42-115/.

the internal workings of the system looking for abnormal or illogical behavior. A highly secured monitor notifies the operator when anomalies are detected and the monitor reconfigures the system to continue operations.

E.   VSP PROJECT DESIGN

The project revolved around two overarching requirements for the Virginia State Police.

- Development of a process for determining at the scene of an incident if cyber attack was involved, if so, the capability to capture data and conduct analysis on any recovered data.

- Through analysis of department vehicles determine existing vulnerabilities and recommend needed mitigation strategies to secure police vehicles against cyber attack.

The project targeted the two predominant makes of vehicles in the VSP fleet operated by Troopers on a daily basis. These were the Ford Taurus and the Chevrolet Impala. While the VSP operate a number of different makes and models of motor vehicles these particular models encompass the bulk of vehicles operated by the agency. A 2013 Ford Taurus and a 2012 Chevrolet Impala were identified in the fleet and designated for the project.

Project teams were identified and arrangements were made for the vehicles to be transported to the testing facilities. The University of Virginia took possession of the Ford Taurus, and the MITRE Corporation housed the Chevrolet Impala at their facility in McLean, Virginia.

Joint teams were formed at each location to conduct research, experimentation, and analysis of possible cyber attacks on the project cars. The teams were given specific roles and were designated as attackers or defenders. For UVA, the attackers consisted of research staff at the university and the defenders were personnel from the private cybersecurity firm of Mission Secure, Inc. The MITRE project team consisted of attackers from the MITRE Corporation and defenders from the private security firm of Kaprica.

F.   VSP PROJECT PLAN

The project consisted of a joint briefing conducted at the headquarters of the Virginia State Police on April 28, 2015. During the course of the meeting, all project team members were briefed on the following objectives and related timetables for the exercise:

- Scope and methodology for complete project

- Overview of UVA's System-Aware Cybersecurity for Computer-Controlled Physical System

- Purple Team Discussion: VSP presented a prioritized list of attacks that were a concern to the agency. List initially consisted of twenty-one identified concerns that if successful would result in injury, significant property damage/theft, loss of life for personnel or citizens. Additional attacks were subsequently added bringing the total to twenty-eight. Successful attacks would result in mission degradation or failure to complete public safety mission requirements.

- Red Team Discussion: Discussion regarding how the supplied lists of VSP attack scenarios could be accomplished.

- Blue Team Discussion: Discussion regarding defense mechanisms to include detection, deterrence, defense, and diagnosis of cyber events.

- Scoring Methodology: Discussion on Failure Modes and Effects Analysis (FMEA) as a foundation for a possible scoring methodology.

- Reporting requirements: 30, 60, 90 day reporting cycle, bi-weekly conference calls, cross pollination of teams to see what each team had accomplished and effect learning for both teams.

Table 1.   VSP Attack List

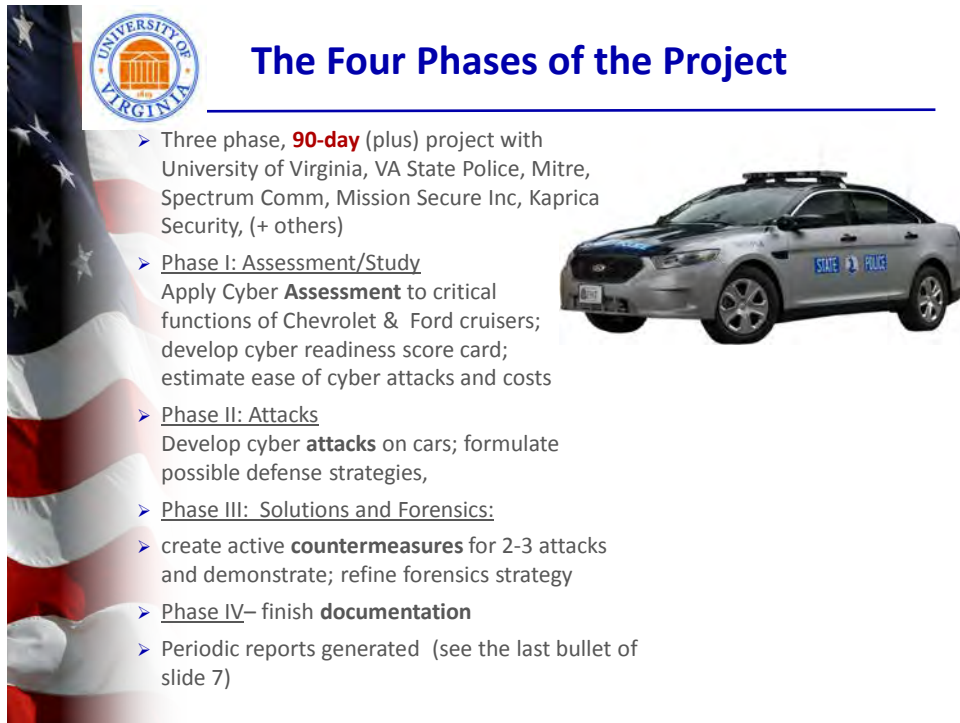| VEHICLE ATTACK	ACTION	CONSEQUENCE
Uncontrolled acceleration to limit	Loss of control	Potential for accident/injury/death to Trooper or civilians
Disengagement of brakes	Loss of control	Potential for accident/injury/death to Trooper or civilians
Asymmetrical braking	Loss of control	Potential for accident/injury/death to Trooper or civilians
Deployment of airbag at speed	Loss of control	Potential for accident/injury/death to Trooper or civilians
Cancellation of all lighting (external & internal) at night	Loss of control	Potential for accident/injury/death to Trooper or civilians
Transmission operation altered	Trooper Stops vehicle	Vehicle removed from service, inability to answer calls
Alter RPM,Throttle, Timing settings	Trooper Stops vehicle	Inability to answer calls for service, vehicle submitted for maintenance
Disengage Electronic Stability Control	Trooper Stops vehicle	Inability to answer calls for service, vehicle submitted for maintenance
Disengage ABS system	Warning Light illuminated	No action required immediately, submitted for service
Shutoff engine no restart	Vehicle stops	Vehicle towed for service, inability to answer calls
Prevent engine from turning off or starting	None	Vehicle removed from service, inability to answer calls
Instrument panel: Falsify readings	Trooper Stops vehicle	No traffic enforcement activity, removed from service
Door Locks activated continuously	None	Inability to answer calls for service, vehicle submitted for maintenance
Unlock Doors	Attempt to secure vehicle	Theft of firearms, radio, and other equipment
Unlock Trunk	Attempt to secure vehicle	Theft of firearms, radio, and other equipment
Lower windows	Attempt to secure vehicle	Theft of property, possible damage from elements
Horn Blows continuously	Remove vehicle from service	Inability to answer calls for service, vehicle submitted for maintenance
Heat / Air conditioning activated continuously	Remove vehicle from service	Inability to answer calls for service, vehicle submitted for maintenance
Car Radio On with increase volume	Remove vehicle from service	Inability to answer calls for service, vehicle submitted for maintenance
Wiper / Washer activated continuously	Remove vehicle from service	Inability to answer calls for service, vehicle submitted for maintenance
Wiping Code	None	No Forensic Investigation capability

G.   PHASES OF VSP PROJECT

The project was to be completed in four phases over an approximate 90-day period as presented by Dr. Thomas Richardson of the University of Virginia.[372] The four phases included:

- Phase I: Assessment/Study

- Phase II: Attacks

- Phase III: Solutions/Forensics

- Phase IV: Reporting

---

372 Dr. Thomas R. Richardson, University of Virginia, PowerPoint presentation, bi-weekly teleconference VSP Cyber project, in possession of the author, August 6, 2015.

Figure 6.   Phases of VSP Project

Source: Dr. Thomas R. Richardson, University of Virginia, PowerPoint presentation, bi-weekly teleconference VSP Cyber project, in possession of the author, August 6, 2015.

The assembled projects teams worked beyond the 90-day window as more attention was received regarding the project and the possibility of presenting the projects findings at a public cybersecurity showcase event arose.

The objectives for the project included detailed study of the electrical architectures of both vehicles to understand data flows across the CAN buses. Wiring diagrams of both systems from the manufacturers were used for this process. In order to understand the actual data flows that instruct the CAN bus to signal micro processors within the vehicle to initiate a specific function, for example, unlocking a door, both teams resorted to fuzzing and used commercially available diagnostic product tools in an effort to identify specific data packets. Manufacturers treat this information as proprietary and protect it accordingly. Fuzzing of data requires significant time searching for data and would not be the recommended course of action to provide cyber protections.

99

Each team explored techniques for launching attacks and developed processes for detecting and deterring attacks. Additionally, teams explored options for capturing data forensically to aid in the investigation of cyber related incidents. Teams were also able to recommend next steps for awareness and risk reduction for policy makers.

H.   FINDINGS FROM VSP CYBER PROJECT

During the six-month project both teams were able to conduct various attacks on both vehicles from the original list provided by VSP. It was determined that the VSP does not have connectivity avenues like Bluetooth, WI-FI, or Telematics as an option on their police cruiser packages.

By not activating these options, the agency has reduced potential attack vectors to their vehicles. Their vehicles were determined to be vulnerable however, but attackers would require direct physical access. A number of scenarios present the possibility for direct access to a police vehicle.

They include routine or scheduled maintenance from private vendors performing work on the vehicle. Also, third party installers of add on equipment, or supply chain products that contain embedded malware might be introduced into vehicle systems. Lastly, direct physical access can be achieved by nefarious actors during the course of normal day to day police activity through surreptitious methods.

While this study proved that direct physical access to the vehicle was required policy makers will have to consider future product purchases from manufacturers that might include connectivity or Telematics as standard equipment rather than optional. The U.S. General Services Administration (GSA) recently issued guidance in support of and mandating use of Telematics in GSA leased vehicles.[373] In FY2012, over one billion dollars was spent leasing vehicles by GSA officials.[374]

The ability to launch cyber attacks was specific to each vehicle. The lessons learned on the Ford product could not be replicated using the same data on the Chevrolet.

---

[373] "Federal Fleets to Study Telematics Expansion," accessed October 6, 2015, http://www.gov ernment-fleet.com/news/story/2014/05/gsa-to-study-telematics-use-change-fuel-rate-structure.aspx.

[374] Ibid.

Each team also attempted to launch attacks on different year models of their project cars and found that the attacks could not be replicated on different year models using the same data packets. Production variance in electronic control units and related equipment on varying years contributed to some level of protection. Hackers would have to develop multiple attacks for different years, makes, and models of agency fleets.

A demonstration of attacks on both vehicles was conducted at the VSP Driver Training Track located in Blackstone, Virginia on September 21, 2015. Attendees at the event included all project team members, staff members from the VSP, and cyber security personnel from Ford Motor Company. The demonstrations were videoed from a number of perspectives both internal and external to the vehicles. It is anticipated that the videos will be used for future training plan development by the VSP to raise awareness regarding emerging risks, and implement initial responses that can be put into place immediately. It is also anticipated that results of this project will be shared with other law enforcement and public safety agencies on a national or state level upon request.

A public demonstration was also conducted at the September 30, 2015 Commonwealth of Virginia Cyber Security Unmanned Systems Technology Showcase event.[375]

---

[375] Dr. Tom R. Richardson, University of Virginia, PowerPoint presentation, September 3, 2015.

Figure 7.　Commonwealth of Virginia Cyber Security Unmanned Systems Technology Showcase Event

Source: Dr. Tom R. Richardson, University of Virginia, PowerPoint presentation, September 3, 2015.

This event was used to raise awareness of cyber issues and to support the Governor's directive issued in the May 2015 press release.

A system was identified for risk assessment modeling in order that events could be scored and charted in order to give meaning to the project. Policy makers would use data from the scoring system to make informed decisions regarding security requirements/enhancements for the fleet, future purchasing decisions, and what future steps would need to be implemented.

Mr. Frank Byrum, Chief Scientist for Spectrum Comm, was assigned the scoring task and evaluated the data produced by both teams. He scored both teams separately and scored all attack scenarios, associated detection capabilities, and deterrence efforts. The

forensic solutions that were displayed by involved project team members were also scored.

Initially it was felt that the "Failure Mode and Effects Analysis" would be the risk assessment model used for the project. This was later changed to the "HEAVENS Model" developed by Volvo of Sweden. This model is used in vehicle security and identifies security vulnerabilities in software intensive automobile systems.[376]

The method allows scoring along two axes. One axis measures the impact of what occurred, for example, casualty or financial impact. The other axis is the threat axis and includes a number of user inputted variables. Examples could include the skill level needed to carry out a cyber attack, how likely is it to occur, what hardware / software is needed, and what window of opportunity would an actor need to carry out the attack.[377]

The accumulated data would then be mapped to indicate probability events that could be scored as critical, medium, or low in the associated categories. At the time of this writing the data for the Virginia State Police cybersecurity project has yet to be tabulated and scored.

I.   RECOMMENDATIONS FROM VSP CYBER PROJECT

Review and/or formulate policy for physical inspection of external and internal areas of police vehicles prior to beginning duty. Inspections internal to the vehicle as a minimum would include visual inspection of the OBD-II port located beneath the dashboard in the vicinity of the steering wheel. Any device attached to this port should be considered suspicious and handled as such. Removal and further inspection of the entire vehicle would be warranted if evidence of tampering is indicated.

Immediate steps should be taken to create training videos and lesson plans for cyber security awareness. All members of the police force should receive training in reference to cyber attacks on physical systems. VSP personnel currently receive annual

---

[376] "HEAVENS," accessed October 6, 2015, http://www.sp.se/en/index/research/dependable_systems/
heavens/sidor/default.aspx.

[377] Mr. Frank Byrum, telephone conversation and in discussion with the author, October 6, 2015.

training regarding cyber awareness for computer information systems. The "*Cyber Crime Checklist for Police Chiefs*" created by the International Association of Chiefs of Police should be used as a baseline for reference material and resources for cyber information. Additional information can be obtained on the IACP website at http://www.iacpcybercenter.org/.

All agencies should review organizational structure, and mission requirements to ensure that cybersecurity matters are reflected in the agencies public safety mission and appropriate individuals have responsibility for maintaining subject matter expertise in the field as new developments occur.

Agency managers are urged to participate in the Government Vehicles Cybersecurity Steering Group set to hold a kickoff meeting on October 22, 2015 in Arlington, Virginia. The goal of the group is to provide actionable information on cybersecurity for vehicles operated by federal, state, and local governments.[378] Membership in the group is anticipated to consist of fleet managers, technical experts, researchers, and other stakeholders. The group will

- Gather input and requirements for cybersecurity for government vehicles

- Identify near term solutions that can be deployed rapidly

- Guide longer term government research and development

- Influence work by industry and academia[379]

Law Enforcement agencies are encouraged to participate in the Cybersecurity Information and Sharing Analysis Center for vehicles due to become operational in November 2015.

It is recommended that police agencies partner with the automobile industry, public / private cybersecurity companies, and academia to further research on development of a forensic capability for data extraction and analysis at the scene of investigations related to cybersecurity.

---

[378] Dr. Dan Massey, DHS S&T, e-mail to the author, September 15, 2015.

[379] Ibid.

Agencies should review any existing criminal statutes related to computer trespass and make determinations on future legislation that would include crimes related to cyber hacking of physical systems or computer information systems.

J.   SUMMARY

Cyber security issues are becoming increasingly prevalent in society. Well documented breaches are occurring with dramatic frequency and create the potential for significant financial loss. But the potential for cyber attacks of motor vehicles has the very serious possibility of creating personal injury or death. Ensuring the integrity of networked systems on vehicles belonging to the general public, as well as public safety agencies is a priority.

It is imperative that awareness and visibility of this issue lead to further research and development and the creation of detection, deterrence, and defense mechanisms for consumer use and for fleet protection of public safety vehicles. It is also imperative that a forensic capability be designed that will support the capturing of data and allow for analysis of reported cyber events.

Cyber attacks on motor vehicles must be documented, researched and controlled to protect the general public and ensure public safety mission requirements can be achieved. Successfully limiting the scope of this emerging threat will serve to gain the needed public trust in order for autonomous and connected vehicles to gain user acceptance as a safe, secure platform for transportation.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. THE WAY FORWARD

The entire ground transportation system is on the verge of dynamic change. Every facet of mobility involving motor vehicles will be impacted. Significant change will occur from design to operation to how individuals even relate emotionally to an automobile. All arenas intersecting with transportation will need to be re-evaluated with respect to autonomous and connected vehicle technology.

Even tangential areas like public transportation, public policy, politics, along with environmental impacts, and land use planning will be affected as the technology is rolled out incrementally for consumer purchase. The cascading effects of change are multi-disciplinary and should be thoroughly evaluated by careful consideration of what potential unintended consequences may develop.

Having a working knowledge of the technology will provide a foundation for decision makers to develop a strategy for implementing change within an organization. By understanding the function of autonomy and connectivity, policies and procedures may then be created or adapted to meet business need or in the case of public safety to ensure that mission requirements continue to be met.

These systems are currently being developed separately as they are not reliant upon each other for operations. Connected vehicle technology is government led and heavily regulated while autonomy is less so and reliant upon the private sector for possible deployment. They both have strategic challenges to overcome prior to deployment, but should at some point in the future merge to complement one another and provide maximum societal benefit to the end user.

A.   SYSTEMS OF SYSTEMS

A system can be thought of as interconnected elements achieving a designed purpose.[380] Autonomous vehicle systems use a collection of sensors, radars, and lidars, to sense the vehicle's surroundings, and then execute computer algorithms to operate with little to no input from a driver.[381] In fact, a "driver" in the conventional sense may become a thing of the past.[382] These systems have been under study for decades by academia, car manufacturers, governmental entities, and more recently by private third party aftermarket suppliers.[383]

An interesting observation of the development of autonomous vehicle technology is the notable lack of governmental regulation. The government's use of autonomy is prevalent in military machinery, for example drone and submersible unmanned systems.[384] However, speaking specifically of the nation's ground transportation system, little has been offered in terms of guidance or regulation for the deployment of autonomous systems in the United States.[385]

Contrast that technology now with connected vehicle research and development, which has been heavily shrouded in governmental regulation and control. Connected vehicles will have the ability to communicate with each other, the infrastructure, and personal communication devices like cell phones, tablets, and personal computers.[386]

---

[380] Donella H. Meadows, *Thinking in Systems: A Primer*, ed. Diana Wright (White River Junction, VT: Chelsea Green Publishing, 2008), 27, http://www.amazon.com/Thinking-Systems-Donella-H-Meadows/dp/1603580557/ref=sr_1_1?s=books&ie=UTF8&qid=1442972085&sr=1-1&keywords=thinking+in+systems.

[381] Panos J. Antsaklis, Kevin M. Passino, and S. J. Wang, "An Introduction to Autonomous Control Systems," *IEEE Control Systems* 11, no. 4 (1991): 5–13.

[382] Sven Beiker, "Legal Aspects of Autonomous Driving," *Santa Clara Law Review* 52, no. 4 (December 12, 2012): 1145.

[383] Erico Guizzo, "How Google's Self-Driving Car Works," October 18, 2011, IEEE Spectrum, http://spectrum.ieee.org/automaton/robotics/artificial-intelligence/how-google-self-driving-car-works.

[384] Ozguner, Stiller, and Redmill, "Systems for Safety and Autonomous Behavior in Cars: The DARPA Grand Challenge Experience," 397–412.

[385] Jesse Chang, Thomas Healy, and John Wood, "The Potential Regulatory Challenges of Increasingly Autonomous Motor Vehicles," *Santa Clara Law Review* 52, no. 4 (December 20, 2012): 1423.

[386] "(USDOT) Releases a New Fact Sheet on Planning for the Future of Connected Vehicles and Intelligent Transportation Systems (ITS)."

These vehicles will provide situational awareness to motorists, pedestrians, and even highway maintenance/response personnel in real time, as driving conditions on the highway are monitored and reported by connected vehicles.[387]

This technology is expected to be a major safety enhancement as it is projected to alleviate up to 80 percent of unimpaired crashes on the highway.[388]

Development of a dedicated communications system for vehicles and infrastructure, along with robust security protocols to ensure integrity of the systems are being studied and developed according to specific guidelines provided by federal government regulators.[389] The U.S. Department of Transportation is expected to mandate connectivity in newly manufactured automobiles, which may allow consumers to purchase this technology by the year 2019.[390]

It is vital that law enforcement agencies and their leadership be made aware of the technology and develop a basic level of understanding about what the technology is, what it is capable of, who the critical stakeholders are, and how law enforcement operations, regulations, and future legislation will be impacted by the introduction of this technology into the marketplace.

When autonomous and connected vehicle technology do become available for purchase by consumers there will still exist a significant hurdle to overcome and that is trust.

The automobile has served a central role for society since its development in the early 20th century. It has been the mainstay of transportation for people around the world. The ability to transport products, goods, and services has also expanded this nation's economy and growth.[391]

---

[387] "(USDOT) Releases a New Fact Sheet on Planning for the Future of Connected Vehicles and Intelligent Transportation Systems (ITS)."

[388] Ibid.

[389] "DSRC: The Future of Safer Driving Fact Sheet."

[390] "(USDOT) Releases a New Fact Sheet on Planning for the Future of Connected Vehicles and Intelligent Transportation Systems (ITS)."

[391] Lio, "History of American Roads and the First Federal Highway."

This iconic symbol of freedom for the individual has also been instrumental in urban development and sparked an entire aftermarket in related industries that support vehicles of every class and description. It has impacted nearly every facet of normal day to day living and as a physical system has evolved through research and development continuously since its inception.

The evolutionary process continues today and is set in the very near future to have yet again transformational impacts on the entire ground transportation system.[392] The introduction of autonomous vehicles or self-driving cars could lead to a transformation in the way people use, enjoy, and benefit from the automobile. These vehicles will initially offer driver assistance benefits and will evolve over time into full automation where minimal driver input will be required.[393]

This paper will focus on what people think and feel about the technology and what role ethics will play in the introduction of automation in vehicles. Driving is a social behavior and if machines are to be responsible for managing the driving function decisions on how to achieve that must be approached with ethics in mind. Ethics is interwoven throughout law and public policy.[394]

Numerous questions have arisen about the technology and how it will be accepted by users. Safety considerations are paramount and having a machine do the driving runs counter to the feelings of control that most people enjoy about the experience of driving a car. The idea of having a mechanical device doing the thinking, evaluating, and choosing to respond to complicated scenario's involving driving a motor vehicle on a public highway certainly would give reason to pause. Especially in light of how poorly humans perform behind the wheel.

---

[392] Anderson et al., Autonomous Vehicle Technology: A Guide for Policymakers*: A Guide for Policymakers*, 9.

[393] "Automobile Sensors May Usher in Self-Driving Cars," accessed September 2, 2015, http://www. edn.com/design/automotive/4368069/Automobile-sensors-may-usher-in-self-driving-cars.

[394] United Nations Institute for Disarmament Research, *The Weaponization of Increasingly Autonomous Technologies: Considering Ethics and Social Values* (Geneva, Switzerland, United Nations Institute for Disarmament Research, 2015).

Traffic crash statistics from NHTSA in 2013 reveal that 32,719 people died from car crashes.[395] The total number of reported crashes for the year exceeded 5.6 million.[396] The estimated economic and societal impact of these events was reported by NHTSA in May 2014 to be estimated at 871 billion dollars.[397] A comparison between rural and urban environments shows that 54% of the fatal crashes occurred in a rural setting while 47% happened in urban areas, yet only 19% of the U.S. population lives in a rural area.[398]

The question then becomes can autonomy in motor vehicles diminish these staggering numbers? The causal factors of these crashes must first be identified to see if autonomy will have any effect on traffic safety outcomes.

The key findings from the NHTSA reports reflect that speeding, driving under the influence, and riding unrestrained in a motor vehicle are the major contributors to deaths, injuries, and crashes.[399] All of these identified factors are human enabled, and human controlled. Of the three fundamental components of highway safety; vehicle, highway, and the human operator it is the last one that contains the most variables for control.

Highway designs are fixed with variables occurring only during construction or maintenance. Motor vehicles are designed with operational limits and motor vehicle safety standards that must be complied with to operate safely on the highway. It is the independent, free will thinking human operator with variable skill level that may be largely responsible for the crashes that result in needless personal injury, property damage, and death.

It is exactly those set of circumstances that developers, engineers, programmers, and academics have set out to neutralize with automation in motor vehicles. NHTSA

---

[395] NHTSA, *2013 Traffic Safety Facts DOT*.

[396] Ibid.

[397] "New NHTSA Study Shows Motor Vehicle Crashes Have $871 Billion Economic and Societal Impact on U.S. Citizens."

[398] NHTSA, *2013 NHTSA Traffic Safety Facts : Rural/Urban Comparison* (Washington, DC: National Highway Traffic Safety Administration, 2013), http://www-nrd.nhtsa.dot.gov/Pubs/812181.pdf.

[399] Ibid.

even reports that technology may be able to reduce unimpaired crashes by 80% percent.[400]

Yet, the answers may not be that simple. The engineering designs of these vehicles are complex as various systems work cohesively to let the car know where it is, where it needs to go, and how to safely travel without endangering occupants or violating rules of the road. This process occurs through sophisticated algorithms that are programmed into the car's computer system. It is here that physical systems and human behaviors converge at a crossroad.

The computer programmer must now consider ethics and moral behavior along with safety and legal responsibilities when writing code for execution by a computer in a motor vehicle.

A new field of study has emerged in traffic safety and academic institutions called machine ethics. It is the study of robotics and how machines make decisions based on ethical or moral behaviors written into computer code.

The early attempts at discussing ethics for machines began with Isaac Asimov, a science fiction writer in the early 1940s, who created the three laws of robotics that were to be followed in sequence. Foremost was the requirement to always protect humans, followed by the absolute dictum to always obey orders unless in conflict with the first law, and lastly the edict to preserve themselves unless violating either of the previous laws.[401]

These laws created unforeseen consequences in Asimov's novels which made them entertaining.

What occurs in the real world is framed by legal standards. With autonomous vehicles the legal framework has yet to be clearly defined, therefore some reliance will necessarily come from our moral or ethical frames.[402]

---

[400] NHTSA, *Planning for the Future of Transportation: Connected Vehicles and ITS.*

[401] "Morals and the Machine," June 2, 2012, http://www.economist.com/node/21556234.

[402] Patrick Lin, "The Ethics of Autonomous Cars," The Atlantic, October 8, 2013, 3, http://www.theatlantic.com/technology/archive/2013/10/the-ethics-of-autonomous-cars/280360/.

Clearly, there are a wide range of ethical behaviors that individual's exhibit based on their particular frame of reference. So the question becomes how would you put ethics into a machine, and whose ethics would be used?

Dr. James H. Moor, professor at Dartmouth College's Department of Philosophy in an article entitled, *The Nature, Importance, and Difficulty of Machine Ethics* describes three categories of ethical agents that may serve as guidelines for programmers to consider as ethics in robotics evolves.[403]

- Implicit ethical agent

- Explicit ethical agent

- Full ethical agent[404]

The implicit ethical agent would avoid an unethical outcome due to its internal software programming. Its virtues are established by code and promote ethical behavior. These can be seen in society today in robotic manufacturing processes, in the banking industry with automatic teller machines, and in the aviation field with automatic pilot systems.[405]

But having a motor vehicle strictly obey the law in every instance might also lead to problems, because humans don't obey traffic laws strictly, but rather at times rely on judgment, wisdom, and reasoning. Their obedience to traffic laws is weighted against safety, traffic flow, and other ethical considerations to achieve a balance between order and chaos.[406]

Engineers at Google have even suggested that programmers could add slightly aggressive behaviors into the written code to handle some common situations

---

[403] James M. Moor, "The Nature, Importance, and Difficulty of Machine Ethics," *Intelligent Systems, IEEE* 21, no. 4 (2006): 18–21.

[404] Ibid.

[405] Ibid.

[406] J. Christian Gerdes and Sarah M. Thornton, "Implementable Ethics for Autonomous Vehicles," in *Autonomes Fahren*, ed. Markus Maurer and Sarah M. Thorton (Berlin, Heidelberg: Springer Berlin Heidelberg, 2015), 87–102, http://link.springer.com/10.1007/978-3-662-45854-9_5.

autonomous vehicles might encounter like at congested intersections controlled by stop signs.[407]

The explicit ethical agent would perform analysis of ethical categories and arrive at a conclusion, similar to how computers use software in gaming.[408] Parameters are established and identified by a computer, which then calculates the best response for the given scenario.

The full ethical agent not only makes an explicit judgment, but is able to justify its selection of an outcome just like a human with free will.[409] Some suggest a machine could never have free will or a conscious and therefore could not achieve status as a full ethical agent.[410]

These three categories of ethical agents do illustrate the importance of interweaving a system of ethics into the framework for deployment of autonomous vehicles. If we expect these vehicles to replicate human behavior in how vehicles are operated on the highway, then ethics must enter the formula and future public policy formation.

Even if the ethical hurdles are overcome another problem to solve will be user acceptance of this technology. Driving a motor vehicle can be very stressful as operators interact with one another and rely on social behavior in addition to rules of the road.

Each driver has their own agenda, capability, and skill level, which contribute to the uncertainty, and insecurity felt by humans in transit. There are no guarantees of safety and autonomous vehicles have yet to be fully tested at the upper levels of autonomy where humans are relieved of driving responsibilities.

Trust takes time to develop and when technology is involved a validation and verification stage will most likely aide society to feel trusting of autonomy. Validation occurs when developers and programmers create the technology and test it satisfactorily

---

[407] Guizzo, "How Google's Self-Driving Car Works."

[408] Moor, "The Nature, Importance, and Difficulty of Machine Ethics."

[409] Ibid.

[410] Ibid., 20.

to assure people it will do what is proposed. The verification process will occur as research, development continues, and exacting standards are established and maintained while vigorous independent testing verifies that expectations are met in the laboratory and under real world conditions.

An October 2014 University of Michigan Transportation Research Institute report gauged public opinion on self-driving vehicles. One survey was conducted in the United States, United Kingdom, and Australia and was then expanded by a separate survey conducted in China, India, and Japan.[411]

The survey results indicate that a majority of citizens in each country had heard of the autonomous vehicles. China (87%) had the greatest familiarity with the technology while Japan (57%) had the smallest margin.[412] The United States response indicated almost three quarters of the respondents had heard of the technology.[413]

When asked about their opinion of autonomous vehicles most responded positively, consistent with the previous question, the Chinese rated the highest at 87 percent with Japan at 43 percent having the least favorable impression.[414] Surprisingly, the country with the most negative impression was the United States at sixteen percent.[415]

A majority of responses indicated concern about self-driving vehicles and suggested that human drivers may actually perform better than machines. Doubt was also expressed about vehicles that were not equipped with driver controls and vehicles that would be moving while unoccupied. A majority suggested that while it would be nice to have a vehicle of this nature a similar majority was unwilling to pay extra in all countries except China and India.[416]

---

[411] Brandon Schoettle and Michael Sivak, "A Survey of Public Opinion about Autonomous and Self-Driving Vehicles in the U.S., the UK, and Australia," 2014, http://deepblue.lib.umich.edu/handle/2027.42/108384.

[412] Ibid.

[413] Ibid.

[414] Ibid.

[415] Ibid.

[416] Ibid.

It appears from the survey that most respondents are optimistic about self-driving cars but are cautious when control over their environment is limited or non-existent. Humans like the feeling of being in control and having the ability to make decisions and then follow through with executing those decisions.

Trust and user acceptance for autonomous vehicles should develop as long as self-driving vehicles are shown to be more capable than a human driver. Mistrust and doubt can be overcome with incremental steps of technology as found in current driver assistance system that are the harbingers of autonomy, and many are available today.

Ethics concern fundamental, widely accepted principles that guide human behavior.[417] The solution of creating machine ethics in autonomous vehicles will not come easily. The development of public policy must be aligned with established social values, which also change on occasion as in the case of marijuana and same sex marriages. Unintended consequences must be considered to satisfy due diligence requirements as public policy for this technology is considered and implemented.

B. RECOMMENDATIONS

There is a lack of federal guidance to homeland security practitioners relative to the use of autonomous and connected vehicles. An enormous amount of research is ongoing related to the development and operational deployment of this technology, but little federal perspective has been issued about securing the systems and data from breach by bad actors.

The federal government has the responsibility and authority to standardize cyber security responses.[418] These minimum requirements for cyber security should be enacted to prevent hacking attempts that will surely occur as they have with other government

---

[417] The United Nations Institute for Disarmament Research, *The Weaponization of Increasingly Autonomous Technologies: Considering Ethics and Social Values*.

[418] Richard T. Baker and Jason Wagner, "Policy Pathways to Vehicle Automation: Industry Perspectives on the Role of Public Policy in Autonomous Vehicle Development," in *2013 International Conference on Connected Vehicles and Expo (ICCVE)*, 2013, 431–36, doi:10.1109/ICCVE.2013.6799831.

and private entities.[419] System failures or unavailability caused by cyber attack could result in the loss of property and lives with autonomous vehicles. Vehicles will need solid security methods to ensure vehicle systems cannot be accessed or provided with false information.[420] This has not been a clear focus of attention to date by automobile manufacturers.[421]

Both hardware and software systems will require security enhancements to ensure integrity and mitigation of unauthorized access or alteration. An important element of security includes detection of unauthorized access to data communications with infrastructure by a system user.[422]

Technology has not always shown itself to be the best solution for problems. Less reliance on a human driver and more transference of responsibility to autonomous operation can also create confusion in a driver's mind as to when and under what circumstances they will be required to take over operations.[423]

Drivers will need to be educated on the limitations of autonomy for vehicles and how they can engage and disengage systems. This requirement may result in legislation identifying minimum knowledge standards for users of autonomous functions.

Manufacturers will face substantial backlash should a component fail and injury occur as a result. Individuals will be more likely to take issue with this type of crash as opposed to a crash that they themselves created.

Specific recommendations for governmental and non-governmental agencies are outlined next along with requirements for future research.

---

[419] "2014's Hacking Pain Is Cyber Security's Gain," accessed September 2, 2014, http://www.forbes. com/sites/chrisversace/2014/01/22/2014s-hacking-pain-is-cyber-securitys-gain-for-symc-feye-pawn-keyw-csco-cuda-ftnt-impv/.

[420] Baker and Wagner, "Policy Pathways to Vehicle Automation."

[421] David Shepardson, "Senators Want Answers on Auto Cyberhacking," *Detroit News*, September 16, 2015, http://www.detroitnews.com/story/business/autos/2015/09/16/senators-want-answers-auto-cyberhacking/32497293/.

[422] "Self-Driving Cars Moving into the Industry's Driver's Seat," accessed September 2, 2014, http:// press.ihs.com/press-release/automotive/self-driving-cars-moving-industrys-drivers-seat.

[423] "Lloyds Insurance Report: Overcoming Obstacles for Driverless Cars."

C.   FEDERAL GOVERNMENT

The federal government can take four specific actions in addressing the evolution of autonomous vehicles.

First among them requires NHTSA to compile and publish a uniform set of national standards. This requirement has been identified as critical by automobile manufacturers and academia proponents as well.[424] This action supports the position held by manufacturers that states would unnecessarily legislate a hodgepodge of mandates that would stifle innovation.[425]

Second, vehicle to infrastructure communications are vital to the development of connected and autonomous vehicles. Security of communications infrastructure, for example, roadside equipment used to send signals to vehicles, will require protection from hacking. Attacks on the communications systems could lead to invasions of privacy through tracking the location or driving route of a particular person.[426]

Also false reports of misbehavior from a vehicle, which are generated by a hacker, could lead to revocation of a security certificate, which would remove the driver from the system.[427] To address these concerns Congress must resolve pending insolvency of the Highway Trust Fund, which contributes significantly to research. These funds are also allocated to the states for infrastructure, which is critical to maintaining secure well-defined lanes and markings that are central to the operation of driverless vehicles.[428] Funding must also be appropriated for the Moving Ahead for Progress in the 21st century Act (MAP 21), which funds multiple programs associated with research for autonomous vehicles.[429]

---

[424] "How Autonomous Vehicles Will Shape the Future of Surface Transportation."

[425] Baker and Wagner, "Policy Pathways to Vehicle Automation."

[426] Kim et al., "An Approach to Communications Security for a Communications Data Delivery System for V2V/V2I Safety: Technical Description and Identification of Policy and Institutional Issues."

[427] Ibid.

[428] "Fixing the Highway Trust Fund Requires Spending Existing Funds More Effectively," accessed July 11, 2014, https://www.enotrans.org/eno-brief/fixing-the-highway-trust-fund-requires-spending-existing-funds-more-effectively.

[429] "Who We Are," accessed July 30, 2014, http://www.fhwa.dot.gov/about/.

Third, the Federal Highway Administration (FHWA) is an "agency within the U.S. Department of Transportation that supports State and local governments in the design, construction, and maintenance of the Nation's highway system (Federal Aid Highway Program) and various federally and tribal owned lands (Federal Lands Highway Program)."[430] This agency must move quickly to issue national level guidelines for assisting state departments of transportation with these new technologies.[431] States can ill afford to develop individual mandates, which will run counter to overall program goals.

Finally, the U.S. Department of Homeland Security (DHS) must advance the study of these technologies and assist in policy development.[432] The Science & Technology Directorate within DHS should direct the Homeland Security Advanced Research Projects Agency to begin research initiatives addressing threats and offering strategic solutions for combating nefarious use of autonomous vehicles.

The Cyber Security Division should be fully engaged to proffer recommendations for the security systems to prevent hacking. The U.S. Department of Homeland Security Science and Technology Directorate (DHS S&T), the Cyber Security Division, and the U.S. Department of Transportation Volpe Center (DOT Volpe), and the non-profit research institute SRI International have formed a new Government Vehicle Cybersecurity Steering Group that will meet in October 2015.[433] This group will assess the threat to government vehicles and develop appropriate recommendations for security measures.

The DHS Office of Policy in close cooperation with its own State and Local law enforcement policy office should be directed to generate policy guidelines regarding licensing, operational use, and legal considerations involving autonomous vehicles.

---

[430] "Who We Are."

[431] United States Government Accountability Office, *Intelligent Transportation Systems: Vehicle-to-Vehicle Technologies Expected to Offer Safety Benefits, but a Variety of Deployment Challenges Exist*.

[432] "Organizational Chart," accessed July 11, 2014, http://www.dhs.gov/organizational-chart.

[433] Invitation in possession of author to participate in Government Vehicle Cybersecurity Steering Group Kickoff Meeting, October 22, 2015, Dr. Dan Massey DHS, e-mail to author, September 15, 2015.

D. STATE GOVERNMENT

States are recommended to adhere to the guidance issued by NHTSA concerning automated vehicles.[434] The role of state governments should be limited to enabling legislation that would license and allow operation of level three and level four autonomous vehicles on public highways as recommended by NHTSA.

States through their respective legislative bodies must also modify existing laws, and develop new paradigms for enforcing legal standards on those who use driverless vehicles. Law enforcement agencies, courts, and other transportation officials must adapt current methods to situations whereby artificial intelligence acts on behalf of a human, but carries the same life or death consequences.[435]

States should encourage and engage in discussions on a national level through each state Office of Intergovernmental Affairs to begin preliminary discussion on effective strategies to combat cyber intrusions and protection of infrastructure for wireless communications. By working with DHS Office of Policy effective policy planning and implementation will occur nationwide.

Law enforcement agencies nationwide should partner with the International Association of Police Chiefs (IACP) to develop best practices for effective cyber security for autonomous vehicles. The IACP has issued the 2015 Cyber Crime Checklist for Police Chiefs.[436]

In addition, law enforcement agencies across the nation will maintain responsibility for the investigation of incidents involving autonomous vehicles. Currently forensic capabilities are limited at the scene of an incident. Development of a mechanism to aid in at scene investigation of potential cyber or traffic related incidents is of utmost concern. Accident investigation procedures and related statutory changes to existing

---

[434] "Automated Driving: Legislative and Regulatory Action," accessed July 10, 2014, http://cyberlaw. stanford.edu/wiki/index.php/Automated_Driving:_Legislative_and_Regulatory_Action.

[435] Beiker, "Legal Aspects of Autonomous Driving."

[436] "Chief's Checklist."

criminal and traffic codes should commence immediately with collaboration from legislative and judicial bodies.

E.   VIRGINIA

The Commonwealth of Virginia should closely coordinate actions and continue the standing autonomous vehicle-working group composed of the following agencies: Department of Motor Vehicles (DMV), Department of State Police (VSP), Department of Transportation (VDOT), Virginia Center for Transportation Innovation Research (VCTIR), and the Virginia Tech Transportation Institute (VTTI). The Insurance Institute for Highway Safety (IIHS) should also be made part of the working group to incorporate research on collision avoidance systems and related areas of study.

The Virginia General Assembly should begin discussions in standing committees focused on autonomous and connected vehicle technology.[437] The following committees will have direct responsibilities for input on this technology within the Commonwealth.

The Joint Commission on Technology & Science studies all aspects of technology and science to promote and assist in technology development. The Joint Transportation Committees of both houses consider matters pertaining to laws of motor vehicles, rules of the road, and traffic regulations.

The Virginia State Crime Commission studies, reports, and makes recommendations to legislative bodies and other stakeholders concerning public safety.

The Department of Criminal Justice Services (DCJS) is the agency responsible for the implementation and administration of federal programs for strengthening law enforcement. They set training standards and certify all law enforcement officers in the Commonwealth.[438]

---

[437] "Interim Studies," accessed July 30, 2014, http://studies.virginiageneralassembly.gov/.

[438] "VA DCJS," accessed October 4, 2015, http://www.dcjs.virginia.gov/.

F.   VIRGINIA STATE POLICE

The Virginia Department of State Police (VSP) should develop an internal working group with representation from the Bureau of Field Operations command staff, Training Academy, Bureau of Criminal Investigation, Staff Attorneys, Fusion Center, and Executive Staff to begin preliminary discussions on how the agency will adapt to meet the challenges of connected and autonomous vehicles.

Partnerships should be developed with the VTTI, VCTIR, IIHS transportation safety institutes to develop functional understandings of the technology and maintain subject matter expertise and research and development continues.

Actions should be undertaken to develop policy and training for Troopers and Special Agents in accident investigations, cyber security, and investigations arising from criminal activity involving autonomous and connected vehicles.

The VSP should partner with regional law enforcement academies to create and present courses to local law enforcement agencies concerning the investigation of accidents, cyber crimes, and criminal investigations involving this technology.

The VSP should evaluate the International Association of Chiefs of Police Technology Policy Framework to establish baseline criteria for capturing data from all technology venues. Additionally, the Cyber Crime Checklist for Police Chiefs should be used as a reference tool for all personnel.

The VSP should continue to partner with institutions as identified in the joint Cyber Security Project conducted on the agencies fleet vehicles during 2015. Membership on the Government Vehicle Cybersecurity Steering Group should be maintained as emerging detection, deflection, and forensic capabilities are created.

VSP Executive staff members should be engaged with General Assembly legislative liaison members to discuss the evaluation, and amendment of Virginia statutes which will be impacted by the emergence of autonomy in motor vehicles.

The VSP Fusion Center should be directly connected to the soon to be created (December 1, 2015) Cyber Car Information Sharing and Analysis Center operated by DHS.

VSP personnel manpower in the High Tech Crimes Unit should be increased significantly to man positions in each of the seven State Police Divisions.

VSP will need to continue partnerships with the American Association of Motor Vehicle Administrators, Virginia DMV, Virginia Department of Transportation to coordinate best practices and sharing of information relative to the emergence of autonomous and connected vehicle technology.

G.   OTHER STAKEHOLDERS

Private stakeholders should be incentivized through tax credits and liability limits to advance research and spark innovation. Many global firms with cyber security divisions are viable options for organizing either public-private models for security services, or standalone private entities that provide system security to prevent cyber attack.[439]

Funding for research by academics should be strongly encouraged to compile data and evaluate systems as they are developed. Advances come from strong research and development. This research will ultimately aid in driving down the cost of vehicles as systems become more reliable. Research will also play a significant role in policy development at every level.

H.   FUTURE RESEARCH

Significant research should be continued in the area of privacy concerns over data transmitted through connected and autonomous vehicles. Carefully balancing the privacy rights and civil liberties of individuals with the need for safely and securely enhancing law enforcement capabilities is needed.

---

[439] "Intelligent Transportation Systems."

Also required is a process for law enforcement entities to request data information on connected vehicles, which are subject to investigation. The structure of the communications system has not yet been identified; however, public safety should have a voice in access in order to advance criminal justices purposes. The process for dissemination could be linked to the state Fusion Centers, which have strict controls in place currently for dissemination of data, or released under the authority of a search warrant obtained from an independent judicial authority.

The impact of autonomy on the legal system will also require detailed study as fundamental questions in jurisprudence will arise surrounding changing statutes and statutory definitions for a driver and operating, as well as liability. Were a major crash involving significant injury or loss of life to occur, liability in crashes could shift from operators to manufacturers or third party installers of the equipment necessary for vehicles to operate in an autonomous mode. This fundamental shift will serve as a catalyst for stifling innovation by manufacturers unwilling to expose the company to potential loss.

I.   CONCLUSION

Vehicles are increasingly linked with computer technology, which can revolutionize highway safety and mobility across the nation. In order to realize the benefit, while safeguarding the country, positive steps must be taken to ensure autonomous and connected vehicle systems provide reliable transportation while ensuring the integrity of the communications system.

While it may be another decade before autonomous vehicles are fully developed, the incremental stages of development have reached the point that policies and procedures for handling the security threats associated with the technology should be well underway.

The federal government must provide the framework for standardization of safety requirements for autonomous vehicles and security of communications systems used by them. Funding must be provided for continued research and development to allow for improvements in functionality.

Policy recommendations on cyber security, privacy, and liability should be provided to states for uniformity and to preclude the stifling of innovation. All states should follow NHTSA's policy guidance to date and resist efforts to over legislate testing and operations.

Continued collaboration with other states and the federal government on policy matters is critical and should include policies related to homeland security measures that would protect the technology, people, and property.

Law enforcement agencies will need to adopt new philosophies and training programs as autonomous vehicles are marketed to the public. The Virginia State Police should take a leading role in this responsibility by partnering with the DCJS and vehicle manufacturers to create an awareness curriculum and accident investigation training program for all Virginia agencies. DHS and other homeland security agencies must also maintain the capability to effectively mitigate the threat posed by this emerging technology.

Effective responses to these vulnerabilities will not be found in a single discipline. A collaborative effort across a broad spectrum of fields in engineering, law, and academia will be required.[440] Actions to be addressed by these disciplines include designing fail safe systems to preclude misuse and system failures, examination of existing tort, liability, and constitutional issues, and continued research and development by subject matter experts.[441] This balanced approach will provide comprehensive research and development of all facets of this emerging technology.

---

[440] Beiker, "Legal Aspects of Autonomous Driving," 1145.

[441] Beiker, "Legal Aspects of Autonomous Driving."

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

AASHTO Executive Committee. *AASHTO Connected Vehicle Field Infrastructure Footprint Analysis: Preparing to Implement a Connected Vehicle Future*. Washington, DC: American Association of State Highway and Transportation Officials, 2014. http://stsmo.transportation.org/Documents/Executive%20 Briefing.pdf.

———. *National Connected Vehicle Field Infrastructure Footprint Analysis*. Washington, DC: American Association of State Highway and Transportation Officials, 2013. http://r.search.yahoo.com/_ylt=A0LEVv3jhqFUCAwAUwEPx Qt.;_ylu=X3oDMTBybnV2cXQwBHNlYwNzcgRwb3MDMgRjb2xvA2JmMQR 2dGlkAw--/RV=2/RE=1419900772/RO=10/RU=http%3a%2f%2fssom.transpor tation.org%2fDocuments%2fApplications_Analysis%2520v3%2520july%252020 13.pdf/RK=0/RS=LfSpgJ63mKEdycufT2Vrxeg6eP8-.

AASHTO Journal. "CBO Says Trust Fund Will Need \$85–90 Billion in Added Revenue for Bill Running to June 2021." Accessed June 5, 2015. http://www.aashtojournal. org/Pages/060515CBOestimate.aspx.

———. "Reports Highlight Weakened Federal, State Investment in Roads, Transit Systems." February 27, 2015. http://www.aashtojournal.org/Pages/022715 spendinglevel.aspx.

———. "Trust Fund Advocates Press Congress During Recess to Soon Finish Long-Term Bill." Accessed August 10, 2015. http://www.aashtojournal.org/Pages/ 080715congress.aspx.

———. "Wright Takes States' Case to Capitol Hill as Time Nears for Decisions on Trust Fund." April 17, 2015. http://www.aashtojournal.org/Pages/041715washpolicy. aspx.

About.com Tech. "How Does GPS Work?." December 16, 2014. http://gps.about.com/ od/beforeyoubuy/a/howgpsworks.htm.

American Association of State Highway and Transportation Officials. "A Policy on Geometric Design of Highways and Streets 2001." 2001. http://nacto.org/docs/ usdg/geometric_design_highways_and_streets_aashto.pdf.

———. "News Release." Accessed October 3, 2015. http://www.aashtojournal.org/Pages /NewsReleaseDetail.aspx?NewsReleaseID=1397.

Anita, Kim, Valerie Kniss, Gary Ritter, and Suzanne M. Sloan. "An Approach to Communications Security for a Communications Data Delivery System for V2V/V2I Safety: Technical Description and Identification of Policy and Institutional Issues." November 2011. http://trid.trb.org/view.aspx?id=1131372.

Antsaklis, Panos, J. Kevin M. Passino, and S. J. Wang. "An Introduction to Autonomous Control Systems." *IEEE Control Systems* 11, no. 4 (1991): 5–13.

AutoBlog. "Short-Staffed NHTSA Struggles to Handle Car-Hacking Threats." Accessed October 5, 2015. http://www.autoblog.com/2015/10/02/short-staffed-nhtsa-struggles-to-handle-car-hacking-threats/.

Auto-Theft.info. "Statistics." Accessed October 3, 2015. http://www.auto-theft.info/?page_id=49.

Baker, Richard T., and Jason Wagner. "Policy Pathways to Vehicle Automation: Industry Perspectives on the Role of Public Policy in Autonomous Vehicle Development." In *2013 International Conference on Connected Vehicles and Expo (ICCVE)*, 2013, 431–36. doi:10.1109/ICCVE.2013.6799831.

Barbaresso, Jim, Gustave Cordahi, Dominie Garcia, Christopher Hill, Alex Jendzejec, and Karissa Wright. *Intelligent Transportation Systems ITS 2015–2019 Strategic Plan*. Washington, DC: U.S. Department of Transportation, 2014. http://www.its.dot.gov/strategicplan.pdf.

Beiker, Sven. "Legal Aspects of Autonomous Driving." *Santa Clara Law Review* 52, no. 4 (December 12, 2012): 1145–1156.

Bluetronix. "Ultra-Wideband Technology." Accessed January 1, 2015. http://www.bluetronix.net/Ultra_Wideband_Technology.htm.

BMW. "BMW X5 : Driver Assistance." Accessed July 14, 2015. http://www.bmw.com/com/en/newvehicles/x/x5/2013/showroom/driver_assistance/index.html.

Borenstein, Johann, Bart Everett, Liqiang Feng, and David K. Wehe. "Mobile Robot Positioning-Sensors and Techniques." DTIC, 1997. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA422844.

Briggs, Rachel. *The Kidnapping Business*. London: The Foreign Policy Center, 2001. fpc.org.uk/fsblob/46.pdf.

Bryant Smith. "Managing Autonomous Transportation Demand." *Santa Clara Law Review* 52, no. 4 (December 19, 2012): 1401–1422.

California Department of Motor Vehicles. "First Set of Autonomous Vehicle Regulations Are Now in Effect." Accessed August 28, 2015. https://www.dmv.ca.gov/portal/dmv/detail/pubs/newsrel/newsrel14/2014_61a.

Center for Auto Safety, The. "GAO Study: Vehicle-to-Vehicle Technologies Expected to Offer Safety Benefits, but a Variety of Deployment Challenges Exist." November 2013. http://www.autosafety.org/gao-study-vehicle-vehicle-technologies-expected-tooffer-safety-benefits-variety-deployment-challenge.

Chan, Ching-Yao. "Connected Vehicles in a Connected World." in *VLSI Design, Automation and Test (VLSI-DAT), 2011 International Symposium on* (IEEE, 2011). http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5783569.

Chang, Jesse, Thomas Healy, and John Wood. "The Potential Regulatory Challenges of Increasingly Autonomous Motor Vehicles." *Santa Clara Law Review* 52, no. 4 (December 20, 2012): 1423–1502.

Checkoway, Stephen, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno. "Comprehensive Experimental Analyses of Automotive Attack Surfaces." in *USENIX Security Symposium*, 2011. http://static.usenix.org/events/sec11/tech/full_papers/Checkoway.pdf.

CNET. "A Brief Intro to OBD-II Technology." Accessed October 5, 2015. http://www.cnet.com/news/a-brief-intro-to-obd-ii-technology/.

Cohen, Roy Alan. "Self-Driving Technology and Autonomous Vehicles: A Whole New World for Potential Product Liability Discussion." *Defense Counsel Journal* 82, no. 3 (2015): 321–345.

Coronado, Pedro Daniel Urbina, Horacio Ahuett-Garza, Vishnu-Baba Sundaresan, and Ruben Morales-Menendez. "Development of an Android OS Based Controller of a Double Motor Propulsion System for Connected Electric Vehicles and Communication Delays Analysis." Mathematical Problems in Engineering, accessed December 2, 2014. http://www.hindawi.com/journals/mpe/2014/467165/abs/.

Cullinane, Brian, Philip Nemec, Manuel Christian Clement, Robertus Christianus Elisabeth Mariet, Lilli Ing-Marie Jonsson. "Engaging and Disengaging for Autonomous Vehicles." US9075413 B2, filed July 17, 2014, and issued July 7, 2015. http://www.google.com/patents/US9075413.

CyberWiki. "Automated Driving: Legislative and Regulatory Action." Accessed July 10, 2014. http://cyberlaw.stanford.edu/wiki/index.php/Automated_Driving:_Legislative_and_Regulatory_Action.

Deep Blue. Brandon Schoettle and Michael Sivak. "A Survey of Public Opinion about Autonomous and Self-Driving Vehicles in the U.S., the UK, and Australia." 2014. http://deepblue.lib.umich.edu/handle/2027.42/108384.

Delphi. "Delphi Drive." Accessed July 14, 2015. http://delphi.com/delphi-drive.

Department of Homeland Security. "Organizational Chart." Accessed July 11, 2014. http://www.dhs.gov/organizational-chart.

———. *Presidential Policy Directive 8: National Preparedness*. Washington, DC: Department of Homeland Security, 2011. http://www.dhs.gov/presidential-policy-directive-8-national-preparedness.

DNI. "DNI Clapper Statement for the Record, Worldwide Cyber Threats before the House Permanent Select Committee on Intelligence." Accessed October 5, 2015. http://www.dni.gov/index.php/newsroom/testimonies/209-congressional-testimonies-2015/1251-dni-clapper-statement-for-the-record,-worldwide-cyber-threats-before-the-house-permanent-select-committee-on-intelligence.

Dolgov, Dmitri, Andrew Schultz, Daniel Trawick Egnor, Christopher Urmson. Systems and Methods for Transitioning Control of an Autonomous Vehicle to a Driver, US20140303827 A1, filed April 5, 2013, and issued October 9, 2014, 1. http://www.google.com/patents/US20140303827.

Douma, Frank, and Sarah Aue Palodichuk. "Criminal Liability Issues Created by Autonomous-Vehicles." *Santa Clara Law Review* 52, no. 4 (December 13, 2012): 1157–1169.

Drug Enforcement Administration, Office of Public Affairs. "DEA Fact Sheet." Accessed July 29, 2014. http://www.justice.gov/dea/docs/factsheet.pdf.

Dudek, Gregory, and Michael Jenkin. "Inertial Sensors, GPS, and Odometry." In *Springer Handbook of Robotics*, 477–90. Berlin: Springer, 2008. http://link.springer.com/10.1007/978-3-540-30301-5_21.

Economist. The. "Morals and the Machine." June 2, 2012. http://www.economist.com/node/21556234.

EDN. "Automobile Sensors May Usher in Self-Driving Cars." Accessed September 2, 2015. http://www.edn.com/design/automotive/4368069/Automobile-sensors-may-usher-in-self-driving-cars.

Elmer, Stephen. "BMW Targets 2020 for Self-Driving Cars." *Auto Guide*, February 26, 2013. http://www.autoguide.com/auto-news/2013/02/bmw-targets-2020-for-self-driving-cars.html.

Eno Center for Transportation, The. "Countdown to Mainstreaming of Self-Driving Vehicles accessed July 11, 2014. https://www.enotrans.org/eno-brief/countdown-to-mainstreaming-of-self-driving-vehicles."

———. "Fixing the Highway Trust Fund Requires Spending Existing Funds More Effectively." Accessed July 11, 2014. https://www.enotrans.org/eno-brief/fixing-the-highway-trust-fund-requires-spending-existing-funds-more-effectively.

FBI. "Brief History of the FBI." Accessed August 27, 2015. https://www.fbi.gov/about-us/history/brief-history/brief-history.

———. "Insurance Fraud." Accessed October 3, 2015. https://www.fbi.gov/stats-services/publications/insurance-fraud /insurance_fraud.

———. "National Cyber Security Awareness Month." Accessed October 5, 2015. https://www.fbi.gov/news/stories/2015/october/national-cyber-security-awareness-month/national-cyber-security-awareness-month.

Federal Communications Commission. "FCC Allocates Spectrum 5.9 GHz Range for Intelligent Transportation Systems Uses." Accessed December 31, 2014. http://transition.fcc.gov/Bureaus/Engineering_Technology/News_Releases/1999/nret9006.html.

Federal Highway Administration. "A Summary of Highway Provisions—MAP-21—Moving Ahead for Progress in the 21st Century." Accessed July 16, 2014. http://www.fhwa.dot.gov/map21/summaryinfo.cfm.

———. "MAP-21." Accessed July 11, 2014. http://www.fhwa.dot.gov/map21/.

———. "Office of Highway Policy Information (OHPI)—Highway Finance Data Collection." Accessed July 29, 2014. https://www.fhwa.dot.gov/policyinformation/pubs/hf/pl11028/.

———. "Who We Are." Accessed July 30, 2014. http://www.fhwa.dot.gov/about/.

Federal Motor Carrier Safety Administration. "Motor Carrier Safety Progress Report (as of March 31, 2015)." Accessed August 28, 2015. http://www.fmcsa.dot.gov/safety/data-and-statistics/motor-carrier-safety-progress-report-march-31-2015.

Federal of American Scientists. "Executive Order 13636." Accessed December 1, 2015. http://fas.org/irp/offdocs/eo/eo-13636.htm.

———. "Executive Order 13691." Accessed October 6, 2015. http://fas.org/irp/offdocs/eo/eo-13691.htm.

Federal Register. "Connected Vehicle Pilot Deployment Program; Request for Information." March 12, 2014. https://www.federalregister.gov/articles/2014/03/12/2014-05414/connected-vehicle-pilot-deployment-program-request-for-information.

Federal Times. "Government Operations, Agency Management, Pay & Benefits." Accessed October 5, 2015. http://www.federaltimes.com/story/government/management/blog/2015/09/23/cyber-onslaught-gets-worse/72688016/.

Fehr, Walton, Tom Lusco, Frank Perry, Jim Marousek, Andrew Hamilton, Gunnar Krueger, and D. McNamara. "Southeast Michigan 2014 Test Bed Project for Connected Vehicles: The Next Step toward Deploying ITS." In *Connected Vehicles and Expo (ICCVE), 2013 International Conference on* (IEEE, 2013), 66–70. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6799771.

FHWA Operations. "Public Meeting Seeking Stakeholder Input to Federal Highway Administration's Vehicle to Infrastructure (V2I) Deployment Guidance." Accessed August 10, 2015. http://www.ops.fhwa.dot.gov/resources/news/v2istakeholdermtg.htm.

Forbes. "2014's Hacking Pain Is Cyber Security's Gain." Accessed September 2, 2014. http://www.forbes.com/sites/chrisversace/2014/01/22/2014s-hacking-pain-is-cyber-securitys-gain-for-symc-feye-pawn-keyw-csco-cuda-ftnt-impv/.

"Futurama 1939 New York World's Fair 'To New Horizons' 1940 General Motors 23min." YouTube video, posted by Jeff Quitney, August 7, 2012. https://www.youtube.com/watch?v=1cRoaPLvQx0.

Gerdes, J. Christian, and Sarah M. Thornton. "Implementable Ethics for Autonomous Vehicles." In *Autonomes Fahren*, edited by Markus Maurer and Sarah M. Thorton. 87–102. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015. http://link.springer.com/10.1007/978-3-662-45854-9_5.

Government Fleet. "Federal Fleets to Study Telematics Expansion." Accessed October 6, 2015. http://www.government-fleet.com/news/story/2014/05/gsa-to-study-telematics-use-change-fuel-rate-structure.aspx.

GPS.gov. "'How GPS Works' Poster." Accessed June 8, 2015. http://www.gps.gov/multimedia/poster/.

Grand Idea Studio. "Smart Parking Meters." Accessed September 2, 2014. http://www.grandideastudio.com/portfolio/smart-parking-meters/.

Greenberg, Andy. "Hackers Could Take Control of Your Car. This Device Can Stop Them." *WIRED*, July 22, 2014. http://www.wired.com/2014/07/car-hacker/.

Gressle, Sharon S. *Homeland Security Act of 2002: Legislative History and Pagination Key* (CRS Report Order Code RL31645). Washington, DC: Congressional Research Service, 2002. http://digital.library.unt.edu/ark:/67531/metacrs7490/m1/1/high_res_d/RL31645_2002Nov26.pdf.

Guizzo, Erico. "How Google's Self-Driving Car Works." October 18, 2011, IEEE Spectrum. http://spectrum.ieee.org/automaton/robotics/artificial-intelligence/how-google-self-driving-car-works.

Guo, Nan, Robert C Qiu, Shaomin S Mo and Kazuaki Takahashi. "60-GHz Millimeter-Wave Radio: Principle, Technology, and New Results." *EURASIP Journal on Wireless Communications and Networking* 2007 (2007): 1–8. doi:10.1155/2007/68253.

Han, Kyusuk, Swapna Divya Potluri, and Kang G. Shin. "On Authentication in a Connected Vehicle: Secure Integration of Mobile Devices with Vehicular Networks." in *Cyber-Physical Systems (ICCPS), 2013 ACM/IEEE International Conference on* (IEEE, 2013), 160–69. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6604010.

Harding, John, Gregory Powell, Rebecca Yoon, Joshua Fikentscher, Charlene Doyle, Dana Sade, Mike Lukuc, Jim Simons and Jing Wang. *Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application*. Washington, DC: NHTSA, 2014.

Harris, Mark. "FBI Warns Driverless Cars Could Be Used as "Lethal Weapons."" theGuardian.com, 2014. http://www.theguardian.com/technology/2014/jul/16/google-fbi-driverless-cars-leathal-weapons-autonomous.

Homeland Security. "Cyber Security Division." Accessed December 1, 2015. http://www.dhs.gov/science-and-technology/cyber-security-division.

Hoppe, Tobias, Stefan Kiltz, and Jana Dittmann. "Security Threats to Automotive CAN networks—Practical Examples and Selected Short-Term Countermeasures." *Reliability Engineering & System Safety* 96, no. 1 (January 2011): 11–25. doi:10.1016/j.ress.2010.06.026.

House Committee on Transportation, U.S. House of Representatives. "How Autonomous Vehicles Will Shape the Future of Surface Transportation." Accessed July 6, 2014. http://transport.house.gov/calendar/eventsingle.aspx?EventID=357149.

HowStuffWorks. "HowStuffWorks 'How Driverless Cars Will Work.'" Accessed July 6, 2014. http://auto.howstuffworks.com/under-the-hood/trends-innovations/driverless-car.htm.

I Am the Cavalry. "Five Star Automotive Safety Program." Accessed February 5, 2015. https://www.iamthecavalry.org/domains/automotive/5star/.

IHS Online Pressroom. "Self-Driving Cars Moving into the Industry's Driver's Seat." Accessed September 2, 2014. http://press.ihs.com/press-release/automotive/self-driving-cars-moving-industrys-drivers-seat.

Intelligent Transportation Society of America. "V2I Deployment Coalition Workshop: June 4–5, 2015." Accessed May 20, 2015. http://www.itsa.org/index.php?option=com_forme&fid=103&Itemid=99999.

International Association of Chiefs of Police. "Technology Policy Framework." Accessed July 30, 2014. http://www.theiacp.org/ViewResult?SearchID=2361.

Isidore, Chris. "Injuries in Google Self-Driving Car Accident." *CNNMoney*, July 17, 2015. http://money.cnn.com/2015/07/17/autos/google-self-driving-car-injury-accident/index.html.

Koscher, Karl, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage. "Experimental Security Analysis of a Modern Automobile." (IEEE, 2010), 447–62. doi:10.1109/SP.2010.34.

Law Enforcement Cyber Center. "Chief's Checklist." Accessed October 4, 2015. http://www.iacpcybercenter.org/chiefs/it-security/chiefs-checklist/.

Levinson, David. "Climbing Mount Next: The Effects of Autonomous Vehicles on Society." *Minn. JL Sci. & Tech.* 16 (2015): 787–1011.

Lin, Patrick. "The Ethics of Autonomous Cars." The Atlantic, October 8, 2013. http://www.theatlantic.com/technology/archive/2013/10/the-ethics-of-autonomous-cars/280360/.

Lio, Ada. "History of American Roads and the First Federal Highway." About.com Inventors. Accessed August 27, 2015. http://inventors.about.com/library/inventors/blcar3.htm.

Lowery, Edward W. "Closing the Cyber Gap: Integrating Cross-Government Cyber Capabilities to Support the DHS Cyber Security Mission." Master's thesis, Naval Postgraduate School, 2014. http://calhoun.nps.edu/handle/10945/44608.

Lu, Ning, Nan Cheng, Ning Zhang, Xuemin Shen, and Jon W. Mark. "Connected Vehicles: Solutions and Challenges." *IEEE Internet of Things Journal* 1, no. 4 (August 2014): 289–99. doi:10.1109/JIOT.2014.2327587.

Luft, Gal. "The Logic of Israel's Targeted Killing." *Middle East Quarterly*, January 1, 2003. http://www.meforum.org/515/the-logic-of-israels-targeted-killing.

Macdonald, Iain David Graham. *A Simulated Autonomous Car*. Edinburgh: The University of Edinburgh, 2011. http://www.inf.ed.ac.uk/publications/thesis/online/IM110982.pdf.

Meadows, Donella H. *Thinking in Systems: A Primer*. Edited by Diana Wright. White River Junction, VT: Chelsea Green Publishing, 2008. http://www.amazon.com/Thinking-Systems-Donella-H-Meadows/dp/1603580557/ref=sr_1_1?s=books&ie=UTF8&qid=1442972085&sr=1-1&keywords=thinking+in+systems.

Michigan Department of Transportation and Center for Automotive Research. *International Survey of Best Practices in Connected and Automated Vehicle Technologies 2013 Update*. Ann Arbor, MI: Michigan Department of Transportation & The Center for Automotive Research, 2013.

Microsoft TechNet. "Understanding Digital Certificates." Accessed November 16, 2014. http://technet.microsoft.com/en- us/library/bb123848%28v=exchg.65%29.aspx.

———. "Understanding Public Key Cryptography." Accessed November 16, 2014. http://technet.microsoft.com/en-us/library/aa998077(v=exchg.65).aspx.

Ministry of Land, Infrastructure, Transport, and Tourism. "ITS (Intelligent Transport System) Spot Services|International Transport Forum 2012 Summit." Accessed May 18, 2015. http://www.mlit.go.jp/kokusai/itf/kokusai_itf_000006.html.

Moor, James M. "The Nature, Importance, and Difficulty of Machine Ethics." *Intelligent Systems, IEEE* 21, no. 4 (2006): 18–21.

National Criminal Justice Reference Service. "NCJRS Abstract." Accessed August 7, 2014. https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=189403.

National Highway Traffic Safety Administration (NHTSA). "New NHTSA Study Shows Motor Vehicle Crashes Have $871 Billion Economic and Societal Impact on U.S. Citizens." Accessed July 24, 2014. http://www.nhtsa.gov/About+NHTSA/ Press+Releases/2014/NHTSA-study-shows-vehicle-crashes-have-$871-billion-impact-on-U.S.-economy,-society.

———. "U.S. Department of Transportation Announces Decision to Move Forward with Vehicle-to-Vehicle Communication Technology for Light Vehicles." Accessed July 28, 2014. http://www.nhtsa.gov/About+NHTSA/Press+Releases/2014/US DOT+to+Move+Forward+with+Vehicle-to- Vehicle+Communication+Tech nology+for+Light+Vehicles.

———. "U.S. Department of Transportation Announces Decision to Move Forward with Vehicle-to-Vehicle Communication Technology for Light Vehicles." Accessed July 28, 2014. http://www.nhtsa.gov/About+NHTSA/Press+Releases/2014/US DOT+to+Move+Forward+with+Vehicle-to-Vehicle+Communication+Techno logy+for+Light+Vehicles.

———. "U.S. Department of Transportation Releases Policy on Automated Vehicle Development." May 30, 2013. http://www.nhtsa.gov/About+NHTSA/Press+ Releases/ U.S.+Department+of+Transportation+Releases+Policy+on+Automated+Vehicle+ Development.

Navaz, A. S. Syed, and G. M. Kadhar Nawaz. "Ultra Wideband on High Speed Wireless Personal Area Networkss." *International Journal of Science and Research (IJSR)*. Accessed January 1, 2015. http://www.ijsr.net/archive/v3i8/U0VQMTQx.pdf.

New England Law Review. "'Look Ma, No Hands!' Wrinkles and Wrecks in the Age of Autonomous Vehicles." Accessed August 27, 2014. http://newenglrev.com/volume-46-issue-3/v46b3garza/.

NHTSA. *2013 NHTSA Traffic Safety Facts : Rural/Urban Comparison.* Washington, DC: National Highway Traffic Safety Administration, 2013. http://www-nrd.nhtsa.dot.gov/Pubs/812181.pdf.

———. *Planning for the Future of Transportation: Connected Vehicles and ITS.* Washington, DC, NHTSA, 2015. http://www.its.dot.gov/factsheets/pdf/Planning FutureTransportation_FactSheet.pdf.

———. *2013 Traffic Safety Facts DOT*. Washington, DC: National Highway Traffic Safety Administration, 2013. http://www-nrd.nhtsa.dot.gov/Pubs/812139.pdf.

Ozguner, Umit, Christoph Stiller, and Keith Redmill. "Systems for Safety and Autonomous Behavior in Cars: The DARPA Grand Challenge Experience." *Proceedings of the IEEE* 95, no. 2 (2007): 397–412.

Palodichuk, Sarah Aue. "Driving into the Digital Age: How SDVs Will Change the Law and Its Enforcement." *Minn. JL Sci. & Tech.* 16 (2015): 827–1011.

Paulin, Carlos, Matt Hatton, Emil Berthelsen, Anupam Malhotra, Michael Würtenberger Don Butler, Matt Jones, Henry Bzeih, Digman, Nicolas Nollet, Robert Jagler, and Ian Pearson. *Telefonica Digital Connected Car Report 2013*. London: Telefonica, 2013.

Penn State. "History of Lidar Development|GEOG 481: LIDAR Technology and Applications." Accessed July 10, 2015. https://www.e-education.psu.edu/geog 481/l1_p4.html.

Public Relations Office, Japan. "Highlighting JAPAN." Accessed May 18, 2015. http://www.gov-online.go.jp/eng/publicity/book/hlj/html/201208/201208_03.html.

Rahiman, Wan, and Zafariq Zainal. "An Overview of Development GPS Navigation for Autonomous Car." In *2013 IEEE 8th Conference on Industrial Electronics and Applications (ICIEA)* (2013). http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=& arnumber=6566533.

RFinklea, Kristin M., and Catherine A. Theohary, *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement* (CS Report No. R42547). Washington, DC: Congressional Research Service, 2012. http://mercury.ethz.ch/serviceengine/Files/ ISN/146602/ipublicationdocument_singledocument/653ce4be-1832-448a-a09c-bbebd7d2b08c/en/193706.pdf.

Roads & Bridges. "Connected Vehicles: U.S. DOT Launches Community Resource website for Connected-Vehicle Pilot Programs." Accessed January 6, 2015. http://www.roadsbridges.com/connected-vehicles-us-dot-launches-community-resource-website-connected-vehicle-pilot-programs.

Roads to the Future. "The Smart Road." Accessed August 10, 2015. http://www.roadsto thefuture.com/Smart_Road.html.

Robohub. "Lloyds Insurance Report: Overcoming Obstacles for Driverless Cars." Accessed September 2, 2014. http://robohub.org/lloyds-insurance-report-overcoming-obstacles-for-driverless-cars/.

Root Labs Rdist. "FasTrak Talk Summary and Slides." Accessed September 2, 2014. http://rdist.root.org/2008/08/07/fastrak-talk-summary-and-slides/.

RouteFifty.com. "Short-Term Highway Trust Fund Extensions Complicate Planning for States." Accessed November 30, 2015. http://www.routefifty.com/2015/11/high way-trust-fund-extensions-planning-state-governments/123307/.

SAE International. "J3016: Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems." Accessed October 16, 2014. http://standards.sae.org/j3016_201401/.

SAE International. "J3061 (WIP) Cybersecurity Guidebook for Cyber-Physical Automotive Systems." Accessed October 3, 2015. http://standards.sae. org/wip/j3061/.

Safercar.gov. "NHTSA V2V Communications." Accessed July 28, 2014. http://www.sa fercar.gov/v2v/v2v.html.

"Safety Pilot Model Deployment: Connected Vehicles." 2012. YouTube video, 3:11. Posted by Quentin Weir, July 16, 2012. https://www.youtube.com/watch?v= hVyS6btjxhI&feature=youtube_gdata_player.

SARTRE. "The SARTRE Project." Accessed September 1, 2015. http://www.sartre-project.eu/en/Sidor/default.aspx.

Schlesinger, Robert. "U.S. Population, 2011: 310 Million and Growing." U.S. *News & World Report*, December 30, 2010. http://www.usnews.com/opinion/blogs/robert-schlesinger/2010/12/30/us-population-2011-310-million-and-growing.

Scholastic.com, "Fast Facts: Japan." Accessed May 19, 2015. http://www.scholastic.com/teachers/article/fast-facts-japan.

SCOTUSblog. "Riley v. California." Accessed October 3, 2015. http://www.scotusblog.com/case-files/cases/riley-v-california/.

Segan, Sascha. "3G vs. 4G: What's the Difference?." *PCMAG*. February 10, 2015. http://www.pcmag.com/article2/0,2817,2399984,00.asp.

Sensors Web. "All about Sensors|A Guide to the Use, Applications, and Technology of Sensors." Accessed September 29, 2015. http://www.sensorsweb.com/temperature_sensors.

Shepardson, David. "Senators Want Answers on Auto Cyberhacking." *Detroit News*, September 16, 2015. http://www. detroitnews.com/story/business/autos/2015/09/16/senators-want-answers-auto-cyberhacking/32497293/.

———. "U.S. Urges Google to Focus on Safety in Driverless Test." *Detroit News*, January 21, 2015. Accessed http://www.detroitnews.com/story/business/autos/2015/01/21/google-safety-driverless-test/22116531/.

sleibson321. "Future Cars: The Word from GM at IDC's Smart Technology World Conference|Steve Leibson." Accessed September 2, 2015. http://low-power design.com/sleibson/2011/05/01/future-cars-the-word-from-gm-at-idc%E2%80%99s-smart-technology-world-conference/.

Smith, Bryant Walker. *Automated Vehicles Are Probably Legal in the United States*. Stanford, CA: The Center for Internet and Society (CIS) at Stanford Law School, 2012. http://cyberlaw.stanford.edu/publications/automated-vehicles-are-probably-legal-united-states.

SP Technical Research Institute of Sweden. "HEAVENS." Accessed October 6, 2015. http://www.sp.se/en/index/research/dependable_systems/heavens/sidor/default.aspx.

Systems Engineering Research Center. "Security Engineering—Design Patterns and Operational Concepts." Accessed October 6, 2015. http://www.sercuarc.org/research/research-program-and-projects/security-engineering-design-patterns-and-operational-concepts-tasks-28-42-115/.

Toyota. "All-New Third Generation Toyota Prius Raises the Bar for Hybrid Vehicles—Again." Accessed July 23, 2014. http://toyotanews.pressroom.toyota.com/article_display.cfm?article_id=1759.

Transportation Research Board of the National Academies. *Critical Issues in Transportation 2013*. Washington, DC: Transportation Research Board of the National Academies, 2013. http://onlinepubs.trb.org/Onlinepubs/general/criticalissues13.pdf.

———. "Road Markings for Machine Vision." Accessed October 3, 2015. http://apps.trb.org/cmsfeed/TRBNetProjectDisplay.asp?ProjectID=4004.

Trimble, Tammy E., Richard Bishop, Justin F. Morgan, and Myra Blanco. *Human Factors Evaluation of Level 2 and Level 3 Automated Driving Concepts: Past Research, State of Automation Technology, and Emerging System Concepts*. Blacksburg, VA: Virginia Tech Transportation Institute, 2014.

U.S. Naval Research Laboratory. "Development of the Radar Principle." Accessed July 10, 2015. http://www.nrl.navy.mil/accomplishments/systems/radar/.

United Nations Institute for Disarmament Research. *The Weaponization of Increasingly Autonomous Technologies: Considering Ethics and Social Values*. Geneva, Switzerland, United Nations Institute for Disarmament Research, 2015.

United State Department of Transportation. "Fast Facts." Accessed October 6, 2015. http://its.dot.gov/fastfacts.htm.

———. "Connected Vehicle Frequently Asked Questions." Accessed July 18, 2014. http://www.its.dot.gov/connected_vehicle/connected_vehicles_FAQs.htm.

———. "DSRC: The Future of Safer Driving Fact Sheet." Accessed December 31, 2014. http://www.its.dot.gov/factsheets/dsrc_factsheet.htm.

———. "Intelligent Transportation Systems—Test Beds." Accessed January 6, 2015. http://www.its.dot.gov/testbed/testbed_affiliated.htm.

———. "ITS ePrimer: Module 13." Accessed August 24, 2015. https://www.pcb.its.dot.gov/eprimer/module13.aspx.

———. "ITS Strategic Plan 2015–2019." Accessed June 12, 2015. http://www.its.dot.gov/strategicplan/index.html.

———. "Regulatory Responsibilities and Contacts." Accessed August 24, 2015. http://www.dot.gov/regulations/regulatory-responsibilities-contacts.

———.. "Table 2–17: Motor Vehicle Safety Data." Accessed July 16, 2014. http://www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/publications/national_transportation_statistics/html/table_02_17.html.

———. "Table 3–10: National Transportation and Economic Trends." Accessed July 16, 2014. http://www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/publications/national_transportation_statistics/html/table_03_10.html.

———. "Table 4–28: Annual Wasted Fuel Due to Congestion." Accessed July 16, 2014. http://www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/publications/national_transportation_statistics/html/table_04_28.html.

———. "(USDOT) Releases a New Fact Sheet on Planning for the Future of Connected Vehicles and Intelligent Transportation Systems (ITS)." Accessed June 12, 2015. http://campaign.r20.constantcontact.com/render?ca=0ce83352-2b4b-48af-a6b1-ff7c0970d778&c=77da6f90-5104-11e3-8e6b-d4ae52a4597c&ch=7a7c1c80-5104-11e3-8e6c-d4ae52a4597c.

———. *U.S. Department of Transportation Vehicle Research Program: Vehicle to Vehicle Safety Application Research Plan*. Washington, DC: United States Department of Transportation, 2011.

United States Government Accountability Office. *Federal Information Security: Agencies Need to Correct Weaknesses and Fully Implement Security Programs* (GAO-15-714). Washington, DC: U.S. Government Accountability Office, 2015. http://www.gao.gov/products/GAO-15-714.

———. *Intelligent Transportation Systems: Vehicle-to-Vehicle Technologies Expected to Offer Safety Benefits, but a Variety of Deployment Challenges Exist* (GAO-14-13). Washington, DC: U.S. Government Accountability Office, 2013. http://www.gao.gov/products/GAO-14-13.

University of Michigan. "University of Michigan Mobility Transformation Center." Accessed August 10, 2015. http://www.mtc.umich.edu/partners/government.

Urban Mobility Information. "Annual Urban Mobility Report." Accessed July 29, 2014. http://mobility.tamu.edu/ums/.

Valdes-Dapena, Peter. "Audi Driverless Car Hits 140 Mph." *CNNMoney*, October 17, 2014. http://money.cnn.com/2014/10/17/autos/audi-rs7-driverless-racetrack/index.html.

Vehicle Automation: TRB@Stanford. "Cybersecurity and Resiliency." Accessed September 9, 2014. http://2013.vehicleautomation.org/program/breakouts/cybersecurity.

Virginia Department of Criminal Justice Services. "VA DCJS." Accessed October 4, 2015. http://www.dcjs.virginia.gov/.

Virginia GeneralAssembly.gov. "Interim Studies." Accessed July 30, 2014. http://studies.virginiageneralassembly.gov/.

Virginia Governor—Newsroom. "Governor McAuliffe Announces Initiative to Protect against Cybersecurity Threats." May 15, 2015. http://governor.virginia.gov/newsroom/newsarticle?articleId=8430.

———. "Governor McAuliffe Announces State Action to Protect against Cybersecurity Threats." April 20, 2015. http://governor.virginia.gov/newsroom/newsarticle?articleId=8210.

Virginia Highway Safety Office, Virginia Department of Motor Vehicles. "2011 Virginia Crash Facts." Accessed July 24, 2014. www.dmv.state.va.us/safety/crash_facts/crash_facts_11.pdf.

Virginia State Police. *Facts and Figures Report 2013*. Richmond, VA: Virginia State Police, 2014. http://www.vsp.state.va.us/Annual_Report.shtm.

Virginia Tech News. Virginia Tech. "Virginia Tech Transportation Institute, Partners Test Automated, Connected Vehicles on Interstate." Accessed November 30, 2015. http://www.vtnews.vt.edu/articles/2015/10/101915-vtti-researchtest.html.

Virginia Tech Transportation Institute. "New VTTI Study Results Continue to Highlight the Dangers of Distracted Driving." Accessed July 29, 2014. https://www.vtti.vt.edu/featured/052913-cellphone.html.

———. "Virginia Connected Corridors." Accessed August 10, 2015. http://www.apps.vtti.vt.edu/PDFs/VCC.pdf.

———. "Virginia Tech Transportation Institute and Partners Unveil Virginia Automated Corridors." Accessed August 10, 2015. http://www.vtti.vt.edu/featured/?p=260.

Virginia's Legislative Information System. "§ 19.2-10.2. Administrative Subpoena Issued for Record from Provider of Electronic Communication Service or Remote Computing Service." Accessed November 30, 2015. http://law.lis.virginia.gov/vacode/19.2-10.2/.

———. "§ 19.2-70.3. Obtaining Records Concerning Electronic Communication Service or Remote Computing Service." Accessed November 30, 2015. http://law.lis.virginia.gov/vacode/19.2-70.3/.

———. "§ 46.2-100. Definitions." Accessed August 28, 2015. http://law.lis.virginia.gov/vacode/title46.2/chapter1/section46.2-100/.

———. "§ 46.2-1157. Inspection of Motor Vehicles Required." Accessed August 28, 2015. http://law.lis.virginia.gov/vacode/title46.2/chapter10/section46.2-1157/.

———. "§ 46.2-372. Driver to Report Certain Accidents in Writing; Certification of Financial Responsibility to Department; Supplemental Reports; Reports by Witnesses." Accessed September 1, 2015. http://law.lis.virginia.gov/vacode/title 46.2/chapter3/section46.2-372/.

———. "Virginia Administrative Code—Title 19. Public Safety—Agency 30. Department of State Police Agency Summary." Accessed August 28, 2015. http://law.lis.virginia.gov/admincode/title19/agency30/preface/.

What A Future!!. "Google Driverless Car: Limiting Destination Abilities Will Prevent Its Misuse." May 27. 2014. http://www.whatafuture.com/2014/05/27/google-driver less-car-your-car-will-prevent-its-own-misuse/.

———. "Google Driverless Car—Data Stored in the Car Memory." June 26, 2014. http://www.whatafuture.com/2014/06/26/google-driverless-car-data-stored-in-car-memory/.

———. "Google Driverless Car—The Obstacle Detection Unit." June 6, 2014. http://www.whatafuture.com/2014/06/14/google-driverless-car-the-obstacle-detection-unit/.

Whitehouse.gov. "Presidential Policy Directive—Critical Infrastructure Security and Resilience." Accessed December 1, 2015. https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

Wideberg, Johan, Pablo Luque, and Daniel Mantaras. "A Smartphone Application to Extract Safety and Environmental Related Information from the OBD-II Interface of a Car." *International Journal of Vehicle Systems Modelling and Testing* 7, no. 1 (2012). http://trid.trb.org/view.aspx?id=1138025.

WIRED. "Why The OPM Breach Is Such a Security and Privacy Debacle." June 11, 2015. http://www.wired.com/2015/06/opm-breach-security-privacy-debacle/.

Wolf, Carol. "U.S. Highway Trust Fund Faces Insolvency Next Year, CBO Says." *Bloomberg*, January 31, 2012. http://www.bloomberg.com/news/2012-01-31/u-s-highway-trust-fund-faces-insolvency-next-year-cbo-says.html.

Wolf, Richard. "Justices' Cellphone Privacy Ruling May Have Broad Impact." *USA Today*, July 20, 2014. http://www.usatoday.com/story/news/nation/2014/07/20/supreme-court-cellphone-privacy-nsa-terrorism/12779997/.

INITIAL DISTRIBUTION LIST

1.   Defense Technical Information Center
        Ft. Belvoir, Virginia

2.   Dudley Knox Library
        Naval Postgraduate School
        Monterey, California